Chapter 11

Reputation System Based Trust-Enabled Routing for Wireless Sensor Networks

A. R. Naseer

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/50736

1. Introduction

The issue of secure routing[1] in wireless and mobile computing is a major challenging design factor in different networking aspects. However, the problem gets more complicated when considering infrastructure-less networks that exhibit even more constraints and new types of attacks. Wireless sensor networks (WSN), which is an ad-hoc type of networks, is a clear representative case.

In the continuously and rapidly evolving area of wireless communication, the field of wireless sensor networks (WSN) comes into the picture as a very hot area of research in all its aspects. WSN is a multi-hop network that is actually one type of ad hoc networks. However, WSN draws the special attention of researchers due to the fact that it exhibits more constraints and critical conditions than normal ad hoc networks in terms of power sources, computing capabilities, memory capacity and other factors. This requires different approaches and protocol engineering directions from those applied to normal ad hoc networks.

One special aspect in WSN is the provision of secure routing. As mentioned previously, the nature of WSN complicates the security requirements and adds difficulties in solving security problems. In fact, secure routing in WSN is actually still not captured well in the research field. One main reason is that the design of a routing protocol is biased towards solving the problem of power limitations and reducing communication overhead, while keeping security concerns in a later phase to be integrated with the current routing solutions.

One specific class of security problems in routing aspects in WSN is the exposure to attacks that are related to nodes' activities and behavior in the network. Such attacks cannot be recognized by verifying nodes' identities because most of these attacks are launched by

compromised nodes or insider attacks; i.e. nodes belong to the same network community. Among different approaches in solving this problem, reputation system based solution is one technique that has generated enough interest among WSN research community. Reputation systems attempt to provide security by allowing different nodes to rate each other based on their routing activities and behavior analysis. When a node has an experience profile about its neighbors, it may select the node that it trusts more, and, hence, achieve a secure routing operation.

In this chapter, a reputation system solution for behavioral based attacks at the network layer as a provision of secure routing in WSN is presented.

1.1. Motivation

In this work, we provide a reputation system based solution for routing security in WSN. We believe that such a solution approach is a feasible and applicable solution for the following reasons:

- Conventional security solution such as cryptography can successfully defend against outsiders' attack. The mechanics of such solutions fail when the attack is done by insiders or compromised nodes. Some of such attacks are intentionally performed like the misbehavior of selfish nodes and compromised nodes. Other attacks can be carried-out unintentionally by faulty nodes [2]. Thus, security systems like reputation based security solutions that have a mechanism to treat such attacks by behavior analysis are more suitable. This is especially true in networks where such misbehavior is very possible or even it is the dominant type of attacks, which is the case in WSN.
- In contrast to different secure routing mechanisms, reputation based systems provide a means for an adaptive and dynamic decision making and reaction at the individual node level behavior. Such features are needed in networks that exhibit dynamicity in nodes' behavior like that in WSN.
- Most WSN deployments and applications invite a very dynamic networking nature. The current conditions and statistics of the network will change from time to time. The security system, thus, must accept to tune itself to these changes at the network level.
- WSN life and operation depends on the cooperation of nodes like any other ad hoc network. This implies that the security interest of a node is not only about itself but also about the whole network. As a result, such networks will prefer to communicate security information in order to keep the network healthy. This is an important feature of reputation systems. Node rating is one type of information that contributes to node's decision making and can be communicated as second hand information. However, the node reaction is also important and affects other nodes' decisions. Thus, the security system should have the feature of a consulted and well-analyzed decision-making and behavior, which are core concepts in reputation systems.
- An interesting and important feature of any reputation system is that it follows a generalized and modular solution approach to fight against any attack in a general framework. The system then is customized to face a subset of these attacks. Thus, new

attacks will be tackled by modifications in the details of the module of interest that does not require a complete system revision. For example, a new attack might require adjusting the monitoring and detection phase without touching other parts of the system. WSN are deployed in very hostile conditions that expect new attempts and attacks. Thus, it is better to support reputation systems in that regard rather than other solutions that can be totally and entirely useless with the occurrence of new misbehavior strategies.

In literature, there are different, proposed reputation based solutions for secure routing in ad hoc networks. Very familiar examples include CONFIDANT (Cooperation Of Nodes – Fairness In Dynamic Ad-hoc Networks) [3], SORI (Secure and Objective Reputation-Based Incentive Scheme for Ad Hoc Networks) [4] and CORE (Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks)[5]. There are also other solutions that are close to the reputation systems but they do not follow the general mechanism. Examples are watchdog and pathrater as well as context-aware detection [6, 7].

As these solutions are applied to ad hoc networks, the conclusion of applying them to wireless sensor network as a type of ad hoc networks is not totally accurate. There are several reasons that show the need to have a special reputation system design and implementation that targets WSN. This differentiation comes from the following facts:

- *Resource Constraints*: An obvious difference between MANET and WSN is resource constraints. Resources include power, memory and processing capabilities. Although both networks suffer from resources deficiency, WSN are more constrained and limited by such resources, especially in power. Any protocol design and implementation targeting WSN from the physical to the application layer must consider resource usage optimization not as an additional feature in the system but as a main design goal. Therefore, an optimized approach must be considered when designing a reputation system for WSN.
- *Conditions and Applications:* Security conditions in WSN are different from general MANET networking type. As a result, the reputation based security system will be looking at providing solutions that satisfy these conditions that indeed implies different approaches for WSN and MANET as they differ in that aspect. Moreover, the risky environment that comes from the application types in WSN raises a remark of having security models that are different than MANET. What implies is a different view of reputation system for WSN.
- *Underlying Routing Protocol*: In contrast to MANET, DSR (Dynamic Source Routing) as a routing protocol is not the accurate or suitable choice for WSN for several reasons related to resource constraints and efficiency. Moreover, other routing protocols like GPSR (Greedy Perimeter Stateless Routing) [8] and GEAR (Geographic Energy Aware Routing protocol) [9] prove their outperformance compared to DSR. Thus, the implemented reputation systems in WSN should consider the operation of routing protocols that are more applicable than DSR.

1.2. Secure routing problem

Routing is a fundamental operation in almost all types of networks because of the introduction of inter-domain communication. Ensuring routing security is a necessary requirement to guarantee the success of routing operation. When we talk about secure routing, we are concerned with security problems that may occur due to improper actions from an assumed router. These undesired actions can be related either to the router identity or the router behavior. If the router has an undesirable identity or authorization, it is considered as an intruder who might perform serious attacks. Such attacks can be avoided by providing security services that validate the routers' identities. On the other hand, a router that misbehaves in the network by performing undesirable routing operations also contributes to the routing security problem. However, the attacks caused by misbehaving routers can be avoided by mechanisms that validate and evaluate the router behavior in the network.

In WSN, secure routing is more demanding due to the nature of the routing operation in WSN. Since WSN lacks an infrastructure, nodes depend on the cooperation among each other to route their packets. Thus, a router in WSN is simply any node that offers a routing service. This "any node" should be selected such that it will be the most secure choice to route the packet. To come up with a proper routing decision we need to understand first what security goals we are targeting.

1.3. Secure routing goals

Security problems in WSN at the network layer can be related to router identity or router behavior. These two issues highlight two main tasks when we would like to design a secure routing solution [1,10].

- Securing Packet Content: This task is concerned with identity related security problems. The goal of this task is to assure that the packet is not accessed by unauthorized nodes as it travels from the source to the destination. This task can be achieved if we can provide the following services:
  - Data Confidentiality: In this service, only the destination node should be able to access the packet content initiated from the source node. Any intermediate router must not have any access to such information. As we can see here, the access of the packet is restricted to the destination node. Thus, if a node other than the destination accesses the packet, it means that the destination identity has been compromised.
  - Data Integrity: When a destination node receives a message from a source, the destination should be able to detect any change that could occur in the message.

Securing packet content is obtained usually based on the idea of identity trust in which a routing decision is made after verifying that the selected node is authorized and has an acceptable identity according to certain criteria. This is achieved in literature by using crypto-based systems. However, any solution must obey WSN constraints of processing capacity, memory limits and energy consumption.

- Securing Packet Delivery: This task deals mainly with behavior related security problems. Its objective is to guarantee that any packet transmitted will be ultimately received at the target destination. Thus, a misbehaving router node should not be able to drop a packet, misroute a packet or deny the ability of routing of other nodes by denial of service attacks. This task can be interpreted in terms of a security service called data availability.
    - Data Availability: If a node A is authorized to get information from another node B, then node A should acquire this information at any time and without unreasonable delay.

There are different approaches to achieve this second task. However, as the first task, the designer should be aware of the suitability of the solution with WSN tight constraints such as energy scarcity. In this work, we are proposing a solution for securing packet delivery task with an account for energy efficiency. Our solution is based on the concept of behavior trust where nodes should trust the behavior of another node in order to select it as a router. This approach is well-known in literature as trust aware routing.

The rest of the chapter is organized as follows. Section 2 of the chapter provides the relevant background material covering an overview of WSN that includes WSN definition, sensor node structure, applications, etc. As WSN is a class of MANET, the main differences between WSN and MANET will be presented. These differences are explained in a way that emphasizes to the reader how they make WSN an independent research target as compared with MANET. Then we introduce the notion of trust and reputation in social networks, how these concepts can be applied smoothly to Wireless Sensor Networks to mitigate node misbehaviors, illustrate the issues in Modeling and Management of Trust & reputation, highlighting the importance of Trust-Aware Routing, and general concept of reputation systems. This will be followed by a detailed discussion on some of the important related work carried out in the area of Reputation system based trust-enabled routing for WSNs.

Section 3, being the Reputation System Overview section, will provide an overview of the proposed reputation system. The section will start by discussing the general reputation system framework clearly introducing the readers to various components of the Reputation system highlighting the functions to be performed by each component. This is followed by description of our customized reputation system- SNARE (Sensor Node Attached Reputation Evaluator)[82] that fits into the framework guidelines. Reputation-based solution will be discussed as a detection approach by presenting the general concept of reputation systems, followed by suggestions and approaches in reputation system solutions that can fit WSN secure routing requirements. In this section, we briefly describe our proposed monitoring component called Efficient Monitoring Procedure in Reputation Systems (EMPIRE)[84], a new rating approach for reputation systems in WSN called CRATER(Cautious RAting for Trust Enabled Routing)[85] and a simple but strong, independent and representative scale to evaluate reputation systems called *REputaion Systems-Independent Scale for Trust On Routing* (RESISTOR)[85].

In section 4, our enhanced routing protocol that aims to provide a secure packet delivery service guarantee by incorporating the trust awareness concept into the routing decision is presented. Our proposed protocol is called Geographic, Energy and Trust Aware Routing (GETAR) which is an enhanced version of the Geographic and Energy Aware Routing (GEAR) protocol[9]. GEAR is basically a geographic routing protocol in which the next hop is selected based on two metrics: the distance between the next hop and the destination and the remaining energy level the next hop owns. The new contribution in GETAR is to add a third metric in the next-hop selection process, i.e. the risk value of a node that is computed by the rating component, CRATER[85] in our case. In section 5, we present a comparison of our approaches with previous reported work and highlight our main contributions. The chapter finally concludes with a summary and future research directions in this field.

2. Background and literature survey

In this section, some background material is provided. It covers general aspects of WSN and then some specific discussions on routing protocols in WSN. This is followed by a general provision of the most familiar work related to the subject of secure routing, notion of Trust and Reputation, reputation systems and trust aware routing.

2.1. WSN: Definition and applications

Wireless Sensor Network (WSN) is one type of ad hoc networks that consists of a very large number of tiny devices equipped with signal processing circuits, microcontrollers, sensors and actuators and wireless transmitters/receivers. Nodes are deployed either randomly or in a grid-like structure according to the sensing and environmental conditions and requirements [11].

WSNs have different applications; most of them are critical mission applications, for example:

- Military Applications [11,12]
  - Monitoring friendly forces, equipment and ammunition
  - Battlefield surveillance
  - Reconnaissance of opposing forces and terrain
  - Targeting guidance
  - Battle damage assessment
  - Nuclear, biological and chemical (NBC) attack detection and reconnaissance.
- Environmental Applications [13,14,15,16]
  - Tracking the movements of birds, small animals, and insects
  - Monitoring environmental conditions that affect irrigation
  - Earth, and environmental monitoring in marine, soil, and atmospheric contexts
  - Forest fire detection
  - Meteorological or geophysical research
  - Flood detection

    - Pollution study
- Health Applications[17,18,15]
    - Providing interfaces for the disabled
    - Integrated patient monitoring
    - Administration in hospitals
    - Tele-monitoring of human physiological data
    - Tracking and monitoring doctors and patients inside a hospital
- Commercial Applications[17,19,20,15]
    - Managing inventory
    - Monitoring product quality
    - Robot control and guidance in automatic manufacturing environments
    - Interactive museums
    - Monitoring disaster area
    - Smart structures with sensor nodes embedded inside
    - Vehicle tracking and detection

2.2. WSN node structure

The basic structure of WSN is that it is composed of sensor nodes and base stations. Sensor nodes, viewed as communicating parties in WSN, are more than simple sensing devices. In fact, every node holds an embedded system that performs three main functions:

- Sensing: Every node should have the ability to observe and/or control the physical environment.
- Computing: The collected data from physical environment through sensing function is processed to produce beneficial information.
- Communication: Every node should be able to communicate and exchange raw data or processed information among them.

Looking at the above functions, the requirements on the sensor hardware will be as follows [11,12,21,22,23,17]:

- *Sensors/Actuators*: Sensing and actuator units are usually composed of sensors, actuators, and analog to digital (for sensing) and digital to analog (for actuating) converters (ADC/DAC). The analog signals produced by the sensors based on the observed phenomenon are converted to digital signals by the ADC, and then fed into the processing unit or the controller. On the other hand, the digital signals produced by the controller are converted to analog signals by the DAC to feed the actuators.
- *Controller*: The controller consists of a processor and a memory system. The processor manages the procedures that make the sensor node collaborate with the other nodes to carry out the assigned sensing tasks. The memory system stores data, software and application programs required to run the node. Though the higher computational powers are being made available in smaller and smaller processors and controllers, processing and memory units of sensor nodes are still scarce resources. For instance, the

processing unit of a smart dust mote prototype is a 4 MHz Atmel AVR8535 microcontroller with 8 KB instruction flash memory, 512 bytes RAM and 512 bytes EEPROM [24]. TinyOS operating system is used on this processor, which has 3500 bytes OS code space and 4500 bytes available code space

- *Radio transceiver*: The radio transceiver unit is responsible for connecting the node to the network.
- *Power supply unit*: One of the most important components of a sensor node is the power unit. Since the sensor nodes are often inaccessible, power is considered a scarce resource and the lifetime of a sensor network depends on the lifetime of the power resources of the nodes. Power is also a scarce resource due to the size limitations. For instance, the total stored energy in a smart dust mote is of the order of 1 J [25]. It is possible to extend the lifetime of the sensor networks by energy scavenging [26], which means extracting energy from the environment. Solar cells are an example for the techniques used for energy scavenging.
- *Localization Systems; e.g. GPS(Global Positioning System):* Most of the sensor network routing techniques and sensing tasks require the knowledge of location with high accuracy. Thus, it is common that a sensor node has a location finding system like the global positioning system GPS.

2.3. Routing protocols in WSN

- *Data centric Routing*: Data-centric routing protocols have an architecture in which there is a sink that communicates with certain regions to collect data from the sensors located in the selected regions [27]. An example of such protocols is SPIN (Sensor Protocols for Information via Negotiation) [28] which is the first data-centric protocol that considers data negotiation between nodes in order to eliminate redundant data and save energy. Another famous example is Directed Diffusion [29]. In this protocol data is diffused through sensor nodes by using a naming scheme for the data. An enhanced version of Directed Diffusion is Rumor routing [30] that routes the queries to the nodes that have observed a particular event rather than flooding the entire network to retrieve information about the occurring events.
- *Hierarchical Routing*: Hierarchical routing attempts to efficiently maintain the energy consumption of sensor nodes by involving them in multi-hop communication within a particular cluster. Data is then aggregated and fused in order to decrease the number of transmitted messages to the sink[27]. LEACH (Low Energy Adaptive Clustering Hierarchy) [31] is one of the first hierarchical routing approaches for sensors networks in which clusters of the sensor nodes are formed based on the received signal strength. The cluster-heads are then used as routers to the sink. This will save energy since the transmissions will only be done by such cluster heads rather than all the sensor nodes. Other protocols are mainly inspired by this protocol, such as TEEN (Threshold sensitive Energy Efficient sensor Network protocol) [32] that is designed to be responsive to sudden changes in the sensed attributes such as temperature.

- *QoS-based Routing*: QoS-aware protocols consider end-tuned delay requirements while setting up the paths in the sensor network [27]. One famous example is SPEED protocol [33]. The main goal of SPEED is to provide soft real-time end-to-end guarantees. The protocol works by making each node maintain information about its neighbors and uses geographic forwarding to find the paths. In addition, SPEED strives to ensure a certain speed for each packet in the network so that each application can estimate the end-to-end delay for the packets by dividing the distance to the sink by the speed of the packet before making the admission decision.
- *Location-based Routing*: Most of the routing protocols for sensor networks require location information for sensor nodes. In most cases, location information is needed in order to calculate the distance between two particular nodes so that energy consumption can be estimated. Since, there is no addressing scheme for sensor networks like IP-addresses and they are spatially deployed on a region, location information can be utilized in routing data in an energy efficient way [27]. One example of such protocols is GPSR [8], which is a greedy protocol. In this protocol, every node selects the next hop as the closest neighbor to the destination. In case when the node of concern is farther to the destination than all its neighbors (such a case is called the void region case), it uses perimeter forwarding based on the planar graphs concept. This research work adopts another interesting protocol under this category, i.e. GEAR [9].

2.4. WSN vs. MANET

WSN is a kind of ad hoc network. From an abstract network view point, WSN is similar in most of the aspects to ad hoc networks. However, WSN is very special compared to other types of ad hoc network due to the following [12,34]:

- The number of sensor nodes in a sensor network can be several orders of magnitude higher than the nodes in an ad hoc network.
- Sensor nodes are densely deployed.
- Sensor nodes are prone to failures.
- The topology of a sensor network changes very frequently.
- Sensor nodes mainly use broadcast communication paradigm whereas most ad hoc networks are based on point-to-point communications.
- Sensor nodes are limited in power, computational capacities, and memory.
- Sensor nodes may not have global identification (ID) because of the large amount of overhead and large number of sensors.
- *Network terminal features*: In WSN, the nodes are tiny sensor nodes. The word tiny describes the node's size and functionality. Computing capabilities, memory capacity and scarce power resources are all limited and significantly smaller than normal terminals in ad hoc networks, which are mostly of a laptop class.
- *Network environment conditions*: WSN has the characteristic of interacting with the environment through sensing functions. As a result, WSN nodes are intentionally deployed to actively respond to physical conditions in the environment such as temperature, vibrations, acceleration, etc. This phenomenon adds a critical

consideration in WSN compared to other types of ad hoc network in the sense that WSN when deployed it is mainly focused on how to satisfy the environmental conditions.

- *Application specifications*: While normal ad hoc networks can be usually thought as general purpose networks, the whole WSN is built to serve a specific application. Therefore, WSN must satisfy the application requirements in addition to the environment conditions. This complicates the issue of finding general purpose solutions for many aspects in WSN.

2.5. Routing attacks

There are several attacks that target the network layer in WSN. For example, in the black-hole attack, adversary nodes do not forward packets completely, while it selectively forwards some packets in gray-hole attack. Another example is the sybil attack in which a node pretends multiple identities. Thus, such a node can virtually exist in different neighborhoods and drop more packets. Wormhole attack is a collusion based attack in which an agreement between two adversaries is made to perform other attacks like blackhole. In wormholes, one adversary misroutes a received packet and sends it to its partner by faking a good routing decision. A detailed explanation of these attacks and others can be found in [35].

2.6. Trust and reputation

In social networks, Trust and Reputation are generally the two important components which play a major role in establishing relationship between entities which have been studied mainly by social scientists for a long time. All kinds of daily transactions, interactions, and communications in human life are based on trust. In a human social community, trust between two individuals is developed based on their actions over time. When faced with uncertainty, individuals trust and rely on the actions and opinions of others who have behaved well in the past. When affairs are to be handled in social networks, people always consider trust and reputation of concerned parties as prime tools for decision making.

Trust in general is the level of confidence in a person or a thing. More precisely trust can be defined as: “the quantified belief by a trustor with respect to the competence, honesty, security and dependability of a trustee within a specified context” [36, 37]. Reputation is a notion sometimes confused with trust; it is defined as “the global perception about the entity’s behavior norms based on the trust that other entities hold in the entity” [38]. Reputation is the opinion of one person about the other, of one internet buyer about an internet seller, and one WSN node about another. Trust is a derivation of the reputation of an entity. Based on a reputation, a level of trust is bestowed upon an entity. The reputation itself has been built over time based on that entity's history of behaviour, and may be reflecting a positive or negative assessment.

In Wireless Sensor Network routing approaches, Reputation system based trust models borrowed from human societies have been proposed to combat misbehaviors. Nodes establish trust relationships between each other and base their routing decisions not only on geographical or pure routing information, but also on their trust that their neighbors will sincerely cooperate. In the context of WSN, Trust is the confidence of one node on another node that it will perform the given task as expected with full cooperation without any deviation. To evaluate the trustworthiness of its neighbors, a node not only monitors their behavior, i.e., through direct observations also known as First Hand Information(FHI), but may also communicate with other nodes to exchange their opinions , i.e., through indirect observations also known as Second Hand Information(SHI). The methods for obtaining trust information and defining each node's trustworthiness are referred to as trust models. A trust model is mostly used not only for higher layer decisions such as routing [39,40], data aggregation [41], but also for cluster head election [42] and for key distribution [43]. Goal of the trust model is to improve security thereby increasing the throughput, the lifetime and the resilience of a wireless sensor network.

Trust in WSN plays an important role in constructing the network and making the addition or deletion of sensor nodes from a network very smooth and transparent. Trust in WSN has been studied lightly by current researchers and is still an open and challenging field. Trust is an old yet important issue in any networked environment that can solve some problems which lies beyond the power of traditional cryptographic security. A Trust Management System is required to support the decision making processes of the network. Trust management is fundamental to identify malicious, selfish and compromised nodes which have been authenticated. In wireless sensor network, trust management system aids the nodes termed as trustors to deal with uncertainty about the future actions of other participating nodes termed as trustees. By evaluating and storing the reputation of other members, it is possible to calculate how much those members can be trusted to perform a particular task. It has been widely studied in many network environments such as peer-to-peer networks, grid and pervasive computing and so on. However, in reality, sensor nodes have limited resources and other special characters, which make trust management for WSNs more significant and challenging. Various Trust models, Trust evaluation metrics and Trust Management schemes have been reported in the literature[36-59]. Current research on the trust management mechanisms of WSNs have mainly focused on nodes' trust evaluation to enhance the security and robustness. The practical applications of this method include the route, data integration and cluster head vote[44]. Although some existing approaches have played greater roles in improving security of other ad-hoc networks, trust management in WSNs still remains a challenging field.

The trust problem is a *decision problem under uncertainty*, and the only coherent way to deal with uncertainty is through *Probability*. There are several frameworks for reasoning under uncertainty, but it is well accepted that the probabilistic paradigm is the theoretically sound framework for solving decision problems with uncertainty. Some of the trust models introduced for sensor networks employ probabilistic solutions mixed with ad-hoc approaches. The problem of assessing a reputation based on observed data is a statistical

problem. Some trust models make use of this observation and introduce probabilistic modeling that uses a Bayesian updating scheme known as the Beta Reputation System [65] for assessing and updating the nodes reputations. The use of the Beta distribution is due to the binary form of the events considered. For example, RFSN[2] uses a probability model in the form of a reputation system to summarize the observed information (FHI) and share the values of the parameters of the probability distributions as second-hand information(SHI). This shared information is soft data, requiring a proper way to incorporate it with the observed data into the trust model. The step of combining both sources of information is handled differently by different trust models. RFSN uses Dempster-Shafer belief theory model [48], solving it using the concept of belief discounting, and doing a reverse mapping from belief theory to continuous probability. In [49], a new Bayesian fusion algorithm to combine more than one trust component - data trust and communication trust to infer the overall trust between nodes is proposed. The trust value calculated between nodes based on their cooperation in routing messages to other nodes in the network is termed as Communication trust (CT). The trust value calculated based on the actual sensed data of the sensors in WSNs is known as Data trust (DT). As an extension to this work, authors proposed Recursive Bayesian Approach to Trust Management (RBTMWSN)[50] by introducing a new trust model and a Gaussian reputation system(GRSSN) for wireless sensor networks based on a sensed continuous data. In this work, Bayesian probabilistic approach based on the work done in modelling Expert Opinion[51] for mixing second-hand information from neighboring nodes with directly observed information is proposed. Opinions provided by knowledgeable sources are known as experts opinions. Such opinions are modulated by existing knowledge about the experts themselves, to provide a calibrated answer. It allows for the formal incorporation of informed knowledge into a statistical analysis. The probabilistic approach adopted is to consider the opinion given by the expert as soft data that is merged with the hard data according to the laws of probability[52]. In [53], authors proposed a Node Behavioral Strategies Banding Belief Theory of the Trust Evaluation (NBBTE) Algorithm. In this approach, at first, each node establishes the direct and indirect trust values of neighbor nodes by comprehensively considering various trust factors such as packet receive, send, strictness, delivery, consistency and availability, *etc*, and combining these factors together with network security grade, correlation of context time and rewards degree. Next, fuzzy set theory is used to decide the trustworthiness levels in accordance with the fuzzy subset grade of membership functions. Based on the levels of trustworthiness, the basic confidence function of D-S evidence theory[54] is accordingly formed. Finally, using the revised Dempster rules of combination, the integrated trust value of a node is obtained by integrating its trustworthiness of multiple neighbor nodes.

Current research challenge has been in designing an accurate and efficient trust and/or reputation model for distributed and heterogeneous environments[47]. When developing such models, different issues have to be taken into consideration. The problem to be solved here consists of deciding in a distributed environment which entity is the most reliable to interact with, in terms of trust and reputation. That is, having a system where different entities offer some services or goods and other ones are requesting those services, the former

will always look for the best self profit, while the latter will demand the best services with respect to some quality characteristics, properties or attributes. Nevertheless, most of the times it is not feasible or realistic to assume the existence of service level agreements or the presence of a centralized entity or architecture supplying reliable information regarding the actual and current behavior of every service provider in the system. Hence, requesters have to determine on their own which service providers are the best ones according to certain criteria. Under these conditions, trust and/or reputation models are aimed to select the most trustworthy entity all over the system offering a certain service.

2.7. Trust aware routing

2.7.1. Definition

A trust aware routing protocol is a routing protocol in which a node incorporates in the routing decision its opinion about the behavior of a candidate router. This opinion is quantified and called the trust metric. Trust metric should reflect how much a router is expected to behave, for example, forward a packet when it receives it from a previous node.

Obtaining the trust metric is a problem by itself since it requires several operational tasks on observing nodes behavior, exchanging nodes' experience and opinions as well as modeling the acquired observations and exchanged knowledge to reflect nodes trust values. A system that provides these tasks to ultimately output a "rating" or a trust value on nodes is called a reputation system.

To appreciate the concept of trust behavior based routing, we provide in the next section some aspects that highlight the importance of trust aware routing.

2.7.2. Importance

Trust aware routing in WSN is important for both securing obtained information as well as protecting the network performance from degradation and network resources from unreasonable consumption.

Most WSN applications carry and deliver very critical and secret information like in military and health applications. A WSN network infected by misbehaving nodes can misroute packets to wrong destinations leading to misinformation or do not forward packets to their destination leading to loss of information. Such critical application can be very sensitive to these attacks. Having a trust aware routing protocol can protect data exchange, secure information delivery and maintain and protect the value of the communicated information.

Node misbehavior can cause performance degradation as well. For example, non forwarding attacks decrease the system throughput since packets will be retransmitted many times and they are not delivered. Denial of service attacks can increase the packet delay since some nodes acting as routers will be busy in responding to the attack and enforced to delay the processing of other packets. An infected WSN network can be partitioned into different parts that cannot communicate among each other due to non

forwarding attacks. This leads to the demand of increasing the number of sensors or changing the node deployment to return network connectivity. This is very expensive, however, can be avoided if a good secure routing solution is adopted.

Network resources are also affected by misbehaving nodes. For example, Denial of service attacks affect resource availability, whether we consider an offended node as a resource for routing or we consider the availability of data itself. Also, this attack forces offended nodes to consume unnecessary energy on packet reception and processing.

As we can see, the information value and the network performance are directly affected by the security level provided by trust awareness of the routing operation in WSN.

2.8. Reputation systems

A reputation system is a type of cooperative filtering algorithm which attempts to determine ratings for a collection of entities that belong to the same community. Every entity rates other entities of interest based on a given collection of opinions that those entities hold about each other[5,60].

Reputation systems have recently received considerable attention in different fields such as distributed artificial intelligence, economics, evolutionary biology, etc. Most of the concepts in reputation systems depend on social networks analogy. As expected, reputation systems are complex in the sense that they do not have a single notion, but a single system will consist of multiple parts of notions. Thus, comparing reputation systems is, in fact, a very difficult problem. All known trials on such problem were based on qualitative approach. The work in [61] proposes an attempt on comparing reputation systems quantitatively based on game theory. The authors, thus, identify different notions of reputation systems like, contextualization, personalization, individual and group reputation, and direct and indirect reputation.

Reputation systems are often useful in large online communities in which users may frequently have the opportunity to interact with users with whom they have no prior experience. Such cases are clearly applicable to e-commerce applications and on line auctioning sites like eBay[62] and Epinions[63]. Another important field that derives the same concept of enforced interaction among entities that lack priori experience on each other is the field of ad hoc and wireless sensor network. This is because nodes in such networks need to route each others' packets. Thus, a trust relation should exist among themselves.

In the context of MANET and WSN [5, 11, 64], the reputation of a node is the amount of trust the other nodes grant to it regarding its cooperation and participation in forwarding packets. Hence, each node keeps track of each other's reputation according to the behavior it observes, and the reputation information may be exchanged between nodes to help each other to infer the accurate values. There is a trade-off between efficiency in using available information and robustness against misinformation. If ratings made by others are considered, the reputation system can be vulnerable to false accusations or false praise.

However, if only one's own experience is considered, the potential for learning from the experiences of others goes unused, which decreases efficiency.

Any reputation system in the context of MANET and WSN should, generally, exhibit three main functions [1, 65]:

- *Monitoring*: This function is responsible for observing the activities of the nodes of its interest set.
- *Rating:* A node will rate its interest set nodes based on the node's own observation, other nodes' observations that are exchanged among themselves, the history of the observed node and certain threshold values.
- *Response*: Once a node builds knowledge on others' reputations, it should be able to decide about different possible reactions it can take, like avoiding bad nodes or even punishing them.

2.9. Related work

2.9.1. SPINS - Security protocols for sensor networks

SPINS (Security Protocols for Sensor Networks) [24] is a set of security protocols that is optimized for WSN. It is mainly composed of two building blocks: (i) *SNEP (Secure Network Encryption Protocol)*: This protocol provides data confidentiality, two-party authentication and data freshness (ii) *μTESLA (micro version of Timed, Efficient, Streaming, Loss-tolerant Authentication protocol)*: This protocol provides authenticated streaming broadcast.

SNEP provides its features by semantic encryption; however, we can notice that these security services do not have a provision for secure routing. In other words, SNEP is an end to end security protocol and cannot prevent routing misbehavior.

On the other hand, μTESLA provides a secure broadcast communication, which is a common and important communication pattern in almost all WSN applications. μTESLA is developed to meet the special condition of WSN. For example, μTESLA authenticates initial packets using only symmetric keys instead of digital signature. μTESLA obtains routing security by authenticated routing that is achieved by deriving the operation on routing update packets and checking the correctness of the claiming parents by key disclosure.

2.9.2. INSENSE - Intrusion-tolerant routing in wireless sensor networks

INSENS (Intrusion-tolerant Routing in Wireless Sensor Networks)[66] constructs tree-structured routing for wireless sensor networks (WSNs). It aims to tolerate damage caused by an intruder who has compromised deployed sensor nodes and is intent on injecting, modifying, or blocking packets. INSENS incorporates distributed lightweight security mechanisms, including one-way hash chains and nested keyed message authentication codes to defend against routing attacks such as wormhole attack. Adapting to WSN characteristics, the design of INSENS also pushes complexity away from resource-poor sensor nodes towards resource-rich base stations.

2.9.3. SeFER - Secure, flexible, and efficient routing protocol

SeFER (Secure, flexible, and efficient routing protocol for sensor networks)[67] is based on random key pre-distribution mechanism. This mechanism aims to provide an easy way for managing the keys in WSN without using public key cryptography. The protocol assumes non symmetric communication architecture in which a tree of sensor nodes delivers information to a controller according to an inquiry sent into the network. Two nodes may communicate indirectly, but securely over a multiple hop path where each pair of nodes on this path shares a common key. The protocol provides the methods for nodes to securely share their keys and communicate directly so that the efficiency of communication is increased.

In fact, all previously mentioned protocols are crypto based solutions. They can successfully fight against attacks in which an intruder falsifies his identity to be a relay for the source such as sybil attack. However, other attacks like selective forwarding, blackhole and HELLO flooding are still possible especially when the attack is performed by an insider node or a node compromised by an intruder. Moreover, any misbehavior due to selfishness or faulty operational nodes cannot be prevented or even detected.

2.9.4. Watchdog and pathrater

Two extensions to the Dynamic Source Routing (DSR) protocol to mitigate the effects of routing misbehavior in ad-hoc networks were proposed in [6,7], namely the Watchdog and the Pathrater. The watchdog is the monitoring part that is designed to be responsible for detecting only non forwarding misbehavior. This is accomplished by overhearing the transmission of the next node. The node thus is assumed to be in a continuous promiscuous mode. When the attack is detected, the observing node informs the source of the concerned path. In this approach, each node maintains a buffer of recently sent packets; in case the packet is not forwarded on within a certain timeout or the overheard packet is different than the one stored in the buffer, the watchdog increments a failure counter for the node responsible for forwarding the packet. If the counter exceeds a certain threshold, the node is considered as misbehaving and the source is notified.

The pathrater is the component used for reputation. Ratings are kept about every node in the network based on its routing activity and they are updated periodically. Nodes select routes with the highest average node rating. Thus, nodes can avoid misbehaving nodes in their routes as a response. The pathrater combines knowledge of misbehaving nodes with link reliability data to select the route most likely to be reliable. Specifically, each node maintains a rating for every other node it knows about in the network and calculates a path metric by averaging the node ratings in the path, enabling thus the selection of the shortest path in case reliability information is unavailable. Negative path values indicate the existence of one or more misbehaving nodes in the path. If a node is marked as misbehaving due to temporary malfunction or incorrect accusation, a second-chance mechanism is considered, by slowly increasing the ratings of nodes that have negative values or by setting them to a non-negative value after a long-timeout. However, misbehaving nodes can still

transmit their packets as there is no punishment mechanism adopted here. Moreover, no second hand information propagation view is considered which limits the cooperativeness among nodes.

2.9.5. CONFIDANT - Cooperation of nodes – Fairness in dynamic ad-hoc networks

In [3], the authors proposed CONFIDANT, a routing protocol for MANET with predetermined trust, and later improved it with an adaptive bayesian reputation and trust system and an enhanced passive acknowledge mechanism (PACK) in [68] and [69] respectively. It is a reputation based secure routing framework in which nodes monitor their neighborhood and detect different kinds of misbehavior by means of an enhanced PACK mechanism. The nodes use the second-hand information from others as a resource of rating, as well. The protocol is based on Bayesian estimation that aims to classify other nodes as misbehaving or normal. The observing node excludes misbehaving nodes from the network as a response, by both avoiding them for routing and denying them cooperation.

In this approach, Upon detection of the node's malice, its packets are not forwarded by normally behaving nodes, while it is avoided in case of a routing decision and deleted from a path cache. CONFIDANT architecture comprises 4 components residing on each node: the Monitor, the Reputation System, the Path Manager and the Trust Manager components. The Monitor component enables nodes to detect deviations of the next node on the source route by either listening to the transmission of the next node ("passive acknowledgement") or by observing route protocol behaviour. In order to convey warning information in case of identification of a bad behaviour, an ALARM message is sent to the Trust Manager component, where the source of the message is evaluated. The rating is updated only if there is sufficient evidence of malicious behaviour that is significant for a node and that has occurred a number of times, exceeding a threshold to rule out coincidences (e.g., collisions). Evidence could come either from a node's own experiences through the Monitor system or from the Trust Manager in the form of Alarm messages. Second-hand information is attributed with low significance (by means of a constant weighting factor w) with respect to the first-hand information, irrespective of its source node. Local rating lists and/or black lists are maintained at each node and potentially exchanged with friends. Black lists may be used in a route request, so as to avoid bad nodes along the way to the destination or to not handle a request originating from a malicious node and in forward packet requests, so as to avoid forwarding packets for nodes that have bad rating.

The protocol assumes a Dynamic Source Routing (DSR) operational routing protocol and lacks a provision on WSN constraints and conditions as it is designed for general ad hoc networks.

2.9.6. CORE - Collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks

Another famous reputation mechanism in literature is CORE protocol (Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks) [5]. It is

a complete reputation mechanism that defines three different types of reputation: (i) Subjective Reputation - reputation observed locally by a node with regards to other nodes (direct observations), (ii) Indirect Reputation - reputation provided by nodes to other nodes which includes only the positive reports by others and (iii) Functional Reputation - also referred as task-specific behavior, which are weighted according to a combined reputation value that is used to make decisions about cooperation or gradual isolation of a node. That is, Subjective Reputation and Indirect Reputation are merged by means of a weighted combining formula in order to compute a final value of reputation concerning a specific evaluation criterion (e.g. packet forwarding) forming Functional Reputation, the last type of reputation considered. By combining different functional reputation values concerning different evaluation criteria, a global reputation value may be estimated. The subjective reputation is computed by giving more relevance to past observations than to recent ones. Subjective Reputation values are updated on the basis of a Watchdog mechanism, if misbehaviour is identified. Indirect Reputation values are updated by means of a reply message that contains a list of all entries that correctly behaved in the context of each function.

In this work, distribution of positive ratings is allowed so as to avoid potential denial of service attacks. In case reputation of an entity is negative, the execution of any requested operation will be denied by all other entities in the system. The system assumes a DSR routing in which nodes can be requesters or providers. The rating is done by comparing the expected result with the actually obtained result of a request. Here, nodes exchange only positive reputation information. The authors argue that this prevents a false-negative (badmouthing) attack, but do not address the issue of collusion to create false praise. In CORE, members have to contribute on a continuing basis (thereby enforcing node cooperation) to remain trusted or they will find their reputation deteriorating until they are excluded. CORE does not provide for a second-chance mechanism.

2.9.7. SORI - Secure and objective reputation-based incentive scheme for ad hoc networks

SORI Scheme for Ad Hoc Networks) [4] targets only the non forwarding attack. SORI monitors the number of forwarded packets from neighborhood and the number of forwarded packets to neighborhood. Reputation rating is then acquired by computing the ratio between the two numbers with a consideration for the confidence in the rating proportional to the number of packets that are initially requested for forwarding. Second hand information is delivered only to the immediate neighbors. This rating source; however, is weighted by what is called credibility, which is derived from the rating ratio. The delivery of the second hand information is achieved by hash-chain based authentication. SORI consists of three components, namely, neighbour monitoring (used to collect information about packet forwarding behaviour of neighbours), reputation propagation (employed so as to share information of other nodes with neighbours) and punishment (involved in the decision process of dropping packet action, taking into account the overall evaluation record of a node and a threshold so as to consider collision events). Reputation rating formation considers first-hand information weighted by a confidence value used to describe how

confident a node is for its judgement on the reputation of another node and second-hand information weighted by the credibility of nodes which contribute to the calculation of reputation. Credibility of a node is defined on the basis of a node's behaviour as forwarder and not as a witness. Reputation rating itself is based on packet forwarding ratio of a node. SORI does not discriminate between selfish and misbehaving node. SORI does not comprise a second-chance / redemption mechanism. Finally, SORI, in order to tackle with impersonation threats, constructs an authentication mechanism based on a one-way-hash chain.

2.9.8. SAR - Security-aware routing

SAR [70] (Security-Aware Routing) is a protocol derived from AODV and based on authentication and a metric called the hierarchical trust value metric. The hierarchal trust values metric governs routing protocol behavior. This metric is embedded into control packets to reflect the minimum trust value required by the sender. Thus, a node that receives any packet can neither process it nor forward it unless it provides the required trust level presented in the packet. Moreover, this metric is also used as a criterion to select routes when many routes satisfying the required trust value are available.

2.9.9. TRANS - Trust routing for location aware sensor networks

TRANS (trust routing for location aware sensor networks) [72] is a geographic routing protocol (GPSR-based [8]) that provides security services using trust metric. It can be considered as a tight trust-based routing due to its specific targets and assumptions. It basically targets a misbehavior model in which an attacker selectively participates in routing signaling and control packets but drops consistently queries and data packets. The protocol also assumes static sensor networks in which a tight mapping can be done between the nodes' identities and their locations. TRANS assumes a location-centric architecture that helps it in isolating misbehavior and establishing trust routing in sensor networks. As a result of that, the protocol assumes a certain communication model in which a single or multiple sinks initiate communication requests with various locations. During that phase, insecure locations are identified and blacklisted. The trust metric used to judge on location security is calculated based on nodes' experience among each other regarding their identities, link availability and packet forwarding.

2.9.10. RGR - Resilient geographic routing

Resilient Geographic Routing (RGR) protocol [73] is also a trust-based routing protocol that relies on a modified routing operation in GPSR. The basic idea in RGR is to assign an initial trust value for each node. Then, this value is incremented or decremented depending on the forwarding activity of the monitored node using a step function. The source node selects probabilistically a subset among its neighbors to forward its packet. This subset is selected from the node's forwarding set that exhibits trust values greater than a threshold.

2.9.11. Robust reputation system for P2P and mobile ad-hoc networks

The main contribution in this work [68] is its proposal for a distributed reputation system that can handle false disseminated information. Every node maintains a reputation rating and a trust rating about every node that is of interest. The authors use a modified Bayesian approach so that they will accept only a second hand information set that is compatible with the current reputation rating. Also, Trust ratings are updated based on the compatibility of second-hand reputation information with prior reputation ratings. The work avoids exploitation of good behavior that can be incorrectly built over time by introducing a concept of re-evaluation and reputation fading.

2.9.12. RFSN - Reputation based framework for high integrity sensor networks

This work[2] proposes a reputation-based framework for sensor networks (RFSN) where nodes maintain reputation for other nodes and use it to evaluate their trustworthiness. The authors tried to focus on an abstract view that provides a scalable, diverse and a generalized approach hoping to tackle all types of misbehaviors resulting from malicious and faulty nodes. They also designed a system within this framework and employed a Bayesian formulation, using a beta distribution model for reputation representation. RFSN integrates tools from statistics and decision theory into a distributed and scalable framework. Bayesian formulation, specifically a beta reputation system is employed for the algorithm steps of reputation representation, updates, integration and trust evolution. This output metric of trust can be used by a node in several ways. For example, a data reading reported by a node can be weighted by the trust of the node when aggregating data from several nodes, thus reducing the impact of the faulty readings. Additionally, the evolution of trust over time provides an on-line tool to the end-user to detect compromised or faulty nodes. This can help the end-user to take appropriate countermeasures such as replacing the corrupted node or sensor.

The system starts the operation by monitoring. Monitoring mechanism follows the classic watchdog methodology in which a node is assumed to be in a promiscuous mode to overhear neighbors' packets. Monitoring behavioral events can result in either cooperative event, α, in which a node is behaving well or non cooperative behavior, β, in which a node misbehaves. The count of each type is injected into the beta distribution formula as the distribution parameters to calculate the node reputation R. This formula calculates node's reputation based on first hand information. The reputation is updated based on the new monitoring events, second hand information received and according to the age of the current reputation value. Any response action is based on selecting the most trusted node. The trust value of a node that is used for decision making is calculated as the statistical expectation of the reputation value.

2.9.13. DRBTS - Distributed reputation-based beacon trust system

In [74] authors propose a reputation based scheme called Distributed Reputation-based Beacon Trust System (DRBTS) for excluding malicious Beacon Nodes(BNs) that provide

false location information. It is a distributed security protocol aimed at providing a method by which BNs can monitor each other and provide information so that the Sensor Nodes(SNs) can choose who to trust, based on a quorum voting approach. In order to trust a BN's information, a sensor must get votes for its trustworthiness from at least half of their common neighbor(s). In this approach, every BN monitors its 1-hop neighborhood for misbehaving BNs and accordingly updates the reputation of the corresponding BN in the Neighbor-Reputation-Table (NRT). The BNs then publish their NRT in their 1-hop neighborhood. BNs use this second-hand information published in NRT for updating the reputation of their neighbors after it qualifies a deviation test. On the other hand, the SNs use the NRT information to determine whether or not to use a given beacon's location information, based on a simple majority voting scheme.

Each BN is responsible for monitoring its neighborhood. When a sensor within its range asks for location information, it responds with its location, as do all other beacon nodes within the range of the requesting node. Due to the promiscuity of broadcast transmissions, a BN can overhear the responses of other BNs in its area. It can then determine its location using this claimed location of each BN and comparing them against its true location. If the difference is within a certain margin of error, then the corresponding BN is considered benign, and its reputation increases. If the difference is greater than the margin of error, then that BN is considered malicious and its reputation is decreased. This distributed model not only alleviates the burden on the base station to a great extent, but also minimizes the damage caused by the malicious nodes by enabling sensor nodes to make a decision on which beacon neighbors to trust, on the fly, when computing their location.

2.9.14. OCEAN - Observation based cooperation enforcement in ad hoc networks

OCEAN[75] approach to selfishness in ad-hoc networks is to disallow any second-hand information exchanges. Instead, a node makes routing decisions based solely on direct observations of its neighbouring nodes' interactions with it. OCEAN is designed on top of DSR protocol, may reside on each node in the network and hosts five components: Neighbour Watch (in order to observe the behaviour of the neighbours of a node), Route Ranker (estimating and maintaining ratings for each of the neighbouring nodes), Rank-based Routing (so as to avoid routes containing nodes in the faulty list), Malicious Traffic Rejection (rejecting all traffic from nodes it considers misleading so that a node is not able to relay its own traffic under the guise of forwarding it on somebody else's behalf) and Second Chance Mechanism (using a time-out based approach for removing a node from a faulty list after a fixed period of observed inactivity and assigning to it a neutral value). Once the rating of a node falls below a certain threshold, the node is added to the faulty list comprising all misbehaving nodes. In order to tackle selfish behaviour, the authors introduce a simple packet forwarding economy scheme, relying again only on direct observations of interactions with neighbours.

Due to the usage of only first-hand information, OCEAN is more resilient to rumour spreading. Finally, the authors rely on recent work on proof-of-effort mechanisms and

mandate that a new identity will be accepted only if the owner shows reasonable effort in generating that identity.

2.9.15. TIBFIT - Trust index based fault tolerance for arbitrary data faults in sensor networks

In [76], authors propose a protocol called TIBFIT to diagnose and mask arbitrary node failures in an event-driven wireless sensor network. An event driven model of behaviour for sensing finds many applications in civilian, military as well as industrial scenarios. The goal of the proposed TIBFIT protocol involves event detection and location determination in the presence of faulty sensor nodes, coupled with diagnosis and isolation of faulty or malicious nodes. In this system model, sensor nodes are organized into clusters with rotating cluster heads. The nodes, including the cluster head, can fail in an arbitrary manner generating missed event reports, false reports, or wrong location reports. Correct nodes are also allowed to make occasional natural errors. The accuracy of the system is defined in terms of fraction of instances when an event occurrence is correctly detected, and its location determined within the given error bound. The approach followed by the protocol is to maintain state of the sensing nodes in terms of the fidelity of their previous sensing actions, and use this information in making decisions involving those sensing nodes. Sensor nodes report the occurrence and location of events to a data sink (cluster head), and remain silent otherwise. The data sink then decides on whether the event occurred and were based on the aggregated data. To determine the location of the event, the data sink must aggregate all reports from nodes within the detection radius. In this approach, a new parameter called *trust index* for this aggregation is introduced. Each node is assigned a trust index to indicate its track record in reporting past events correctly. The cluster head analyzes the event reports using the trust index and makes event decisions. The *Trust Index(TI)* of a node is a quantitative measure of the fidelity of previous event reports of that node as seen by the data sink. In a system comprised of sensing nodes, the data sink assigns and maintains a TI for each node in its domain, and does voting in a state-full manner. As the system runs over a longer time, more state is built up concerning the performance of the associated sensing nodes, and hence tolerance for faults also goes up accordingly. Authors claim that TIBFIT can tolerate faults in a network with more than 50% of its nodes compromised *after* it has built up adequate state of the nodes.

The main contributions of this paper are the following:

i. TIBFIT tolerates nodes that fail both naturally and maliciously, and makes decisions on event occurrence as well as location**.** Under several scenarios, accurate event determination and localization can be done even with more than 50% of the network compromised.
ii. No nodes are considered immune to failure, whether they are sensing nodes or the data sink.
iii. An adversary model is proposed with increasing levels of sophistication and demonstrated the effectiveness of the protocol in each case.

iv. The protocol is generic and can be applied to any data sensing and aggregation application in sensor networks.

2.9.16. PLUS - Parameterized and localized trust management scheme protocol

In [77] authors have proposed Parameterized and Localized trUst management Scheme (PLUS) for WSNs. The authors adopt a localized distributed approach and trust is calculated based on either direct observations or indirect observations. Whenever a node needs recommendation about another node, it will broadcast a request packet to its neighbors. This packet contains the identity of the evaluating node. In response all the nodes (except the node whose is going to be evaluated) send back a response packet to the requester. Once all the response packets are received, the requester will calculate the final trust value. If the node finds any misbehavior about the evaluated node, then the node will broadcast a exchange information packet to its neighbors. This packet contains information about identity of the node and error code. Based on the trust policy, the neighboring nodes send out its opinion: exchange Acknowledgement packet in case if they agree with the sender, otherwise neighbors will reply with exchange Argue packet indicating disagreement.

2.9.17. LARS - Locally aware reputation system

In [78], the authors propose LARS to mitigate misbehavior and enforce cooperation. Each node only keeps the reputation values of all its one-hop neighbours. The reputation values are updated on the basis of direct observations of the node's neighbours. If the reputation value of a node drops below an untrustworthy threshold, then it is considered misbehaving by the specific evaluator node. In such a case, the evaluator node will notify its neighbours about misbehaviour, by initiating a WARNING message. An uncooperative node is identified in the neighbourhood region, in case a WARNING message issued by a node is co-signed by m different one hop-neighbours, where $m-1$ is an upper bound on the number of nodes considered in the one-hop neighbourhood, in order to prevent false accusations and problems caused with inconsistent reputation values. Additionally, a fade factor has been introduced to give less weight to evidence received in the past. The misbehaving node is not excluded from the network for ever. After a time-out period, it is accepted, but with the reputation value unchanged so it would have to built its reputation by good cooperation.

2.9.18. TARF - A trust-aware routing framework for wireless sensor networks

In [79] authors propose a trust aware routing framework for WSNs called TARF to secure multi-hop routing in WSNs against intruders exploiting the replay of routing information. This approach identifies malicious nodes that misuse "stolen" identities to misdirect packets by their low trustworthiness, thus helping nodes circumvent those attackers in their routing paths. It incorporates the trustworthiness of nodes into routing decisions and allows a node to circumvent an adversary misdirecting considerable traffic with a forged identity attained through replaying. It significantly reduces negative impacts from these attackers. TARF is also energy efficient, highly scalable, and well adaptable.

In this approach, to route a data packet to the base station, a node only needs to decide to which neighbouring node it should forward the data packet considering both the trustworthiness and the energy efficiency. It maintains a neighbourhood table with trust level values and energy cost values for certain known neighbours. Two types of routing information that need to be exchanged in addition to data packet transmission are – (i) Broadcast messages from the base station about data delivery and (ii) Energy cost report messages from each node. Neither message needs acknowledgement. A broadcast message from the base station is flooded to the whole network. The other type of exchanged routing information is the energy cost report message from each node, which is broadcast to only its neighbours once. Any node receiving such an energy cost report message will not forward it. Each node has two modules – *Energy Watcher* and *Trust Manager* running on it in order to maintain a neighbourhood table with trust level values and energy cost values for certain known neighbours. *Energy Watcher* is responsible for recording the energy cost for each known neighbour, based on nodes observation of one-hop transmission to reach its neighbours and the energy cost report from those neighbours. A compromised node may falsely report an extremely low energy cost to lure its neighbours into selecting this compromised node as their next-hop node; however, these TARF-enabled neighbours eventually abandon that compromised next hop node based on its low trustworthiness as tracked by *Trust Manager*. *Trust Manager* is responsible for tracking trust level values of neighbours based on network loop discovery and broadcast messages from the base station about data delivery. At the beginning, each neighbour is given a neutral trust level. After any of those events occurs, the relevant neighbours' trust levels are updated. Occurrence of a loop degrades that node's next-hop node's trust level thereby gradually taking the trust level to a low value leading to the breaking of the loop by changing its next-hop selection. On the other hand, to detect the traffic misdirection by nodes exploiting the replay of routing information, *Trust Manager* computes the ratio of the number of successfully delivered packets which are forwarded by this node to the number of those forwarded data packets, denoted as Delivery Ratio. Once a node is able to decide its next hop neighbour according to its neighbourhood table, it sends out its energy report message - it broadcasts to all its neighbours its energy cost to deliver a packet from the node to the base station.

2.9.19. SensorTrust - A resilient trust model for wireless sensing systems

In[80], authors propose a resilient trust model, SensorTrust with a focus on data integrity for hierarchical WSNs. In this model, the aggregator maintains trust estimations for children nodes by integrating their long-term reputation and short-term risk and taking into consideration both communication robustness and data integrity. Long-term reputation, also called conventional reputation, refers to its average performance level in its whole past history, and short-term risk identifies to which degree its future behaviour is associated with its recent performance. Neither long-term reputation nor short-term risk alone could fully reflect current trustworthiness. On the one hand, a single fault could occasionally happen to even a trustworthy sensor node, but that doesn't necessarily mean the node is unreliable. That suggests the one-sidedness of short-term risk. On the other hand, long-term

reputation treats the node's behaviour in each transaction equally. But in the real world, a node with good average performance level might begin to behave negatively during recent transactions. That could suggest that the sensor starts to malfunction. Since a node can behave maliciously regarding either wireless communication or data management, trustworthiness is evaluated from two aspects: communication robustness and data integrity. This model employs the Gaussian model to rate data integrity in a fine-grained style, and a flexible update protocol to adapt to different applications. In this model, to accurately identify the current trust level, past history and recent risk are synthesized in a real-time way. This model uses a SensorTrust value, which is a decimal number in [0,1], to represent trustworthiness level. The higher some node's SensorTrust value is, the more trustworthy that node is. Specifically, the SensorTrust value in terms of communication robustness is the estimated probability of a positive communication transaction; the SensorTrust value in terms of data integrity is the estimated probability of integrity of data. At the beginning, the aggregator assigns a SensorTrust value of 0 to its children nodes, since no evidence of trustworthiness is available. Each time a sensor node interacts with its associated aggregator, the aggregator evaluates the node's behavior by giving a rating number in [0,1] for this transaction in terms of communication robustness and data integrity respectively. This rating number reflects the aggregator's opinion of the current transaction: the higher the rating numbering is, the more positive the aggregator views the sensor node to be. The rating number together with its latest SensorTrust value will be used by the aggregator to update the node's SensorTrust value. With acceptable overhead, SensorTrust proves resilient against varied faults and attacks.

Considering the related work reported in the literature, it can be stated that there is a lack of standardization orientations when designing a trust and/or reputation model for distributed systems[46,47,55]. It has been found that approaches/schemes proposed in related research literature are based on quite different assumptions, while the trust/reputation framework considered varies significantly in many aspects. Some of the aspects in which these reported approaches differ can be listed as - Computation of trust/reputation considering only first hand information or both first-hand and second-hand information, Propagation of second-hand information considering only positive, negative or both types of recommendation, Degree of propagation, Adopted model for reputation value computation, Dishonest second-hand information provisioning, Identification of misbehaving nodes, Actions taken, Node re-integration in the system, etc. The proposed reputation systems use several debatable heuristics for the key steps of reputation updates and integration. Some systems maintain a statistical representation of the reputation by borrowing tools from the realms of game theory. These systems try to counter selfish routing misbehaviour of nodes by enforcing nodes to cooperate with each other. More recent reputation systems proposed in the domain of ad-hoc and sensor networks, formulate the problem in the realm of Bayesian analytics rather than game theory. Furthermore, most of the trust research focuses on communication behaviors without clearly indicating data integrity importance. Some reported recent approaches employ communication trust and data trust separately in their suggested trust models considering the fact that one of the main tasks of WSNs is data collection and moreover, different applications have their own specific requirements regarding communication trustworthiness and data trustworthiness.

3. Reputation system overview

In this section, an overview of the proposed reputation system will be presented. The section will start by describing the general framework. This is followed by a brief description of our customized reputation system that fits into the framework guidelines.

3.1. Reputation system framework

The conceptual operation of the reputation system is based on building a trust relation between different members of the community as they learn about each other. Thus, irrespective of why a node needs to build such relations, any reputation system must have two basic components, i.e. monitoring component to allow nodes to learn about each other and rating component to build the trust relations among nodes. However, the purpose of these trust relations will determine the specifications of each component and may imply a new component responsible for further actions based on the trust relations.

Our reputation system is fully distributed in the sense that each node implements all modules with the full functionality. Moreover, at the initial deployment stage, all nodes start with default and equal reputation values. This implies that all nodes have the same trust relation among each other. However, these initial reputation values are not the ones that imply a full trust. This is because our system assumes an always-suspicious environment in which all nodes are always '*suspects*'. A node can increase its reputation by good behavior or, otherwise, it decreases.

Since the purpose of the reputation system in this work is to provide trust aware routing in WSN, there are three basic components in our system. They are as follows.

3.1.1. Monitoring component

The reputation system operation starts by the execution of monitoring component. Monitoring component is responsible for collecting behavior information by direct observation of neighbor's activities. In this work, we are concerned only in routing activities and, more specifically, in packet forwarding, i.e. monitoring whether a router is forwarding a packet or not. After a monitoring node detects some misbehavior, it reports its observation as a quantity to the rating component.

3.1.2. Rating component

This component is responsible for evaluating the reputation of an observed node. Assume that node A wants to evaluate a reputation value for a node B that may or may not be directly monitored by A. Then, the reputation value of B evaluated by A is a number that reflects how good or bad node B behaves from the perspective of node A considering:

- Monitoring results of all types of routing activities.
- Monitoring results obtained by direct observations from A as first hand information, if any.

- Monitoring results gathered from other nodes observing B and shared with A as second hand information, if any.

Once a reputation value for B is formed by A, A will decide about a certain level of trust relationship with B. Notice that, according to these specifications of the rating module, it is not necessary that A and B are neighbors to each other. Thus, A can have a trust relation with any node in the network. This, in fact, helps in generalizing the framework to allow the use of various routing protocols that differ in the obtainable level of hop information. For example, with DSR, in which multi-hop information can be collected, this module provides the ability to build trust relations among all nodes from source to destination. Also, on the other extreme, the module can work with geographic routing protocols like GPSR and GEAR with one hop information.

3.1.3. Response component

Once node A gets reputation knowledge about node B and decides a trust relation with it, A may or may not respond to B's behavior. Since our system treats the secure routing purpose, A should respond in a proper manner. Among different possible reactions provided in many reputation systems [3, 5, 72], our system framework assumes three main response approaches with regard to node A.

- *Defensive approach*: Here, node A just avoids using node B as a router. This avoidance can be gradual as the reputation value of node B decreases. However, B can still use A or any node to forward its packets.
- *Offensive approach*: In this approach, node A avoids B as in the previous approach. In addition to that, A takes further actions by punishing node B. However, node B still has the right to defend itself and is treated normally if it can prove a good behavior.
- *Dismissal approach*: in this approach, node A totally ignores node B as if it is not in the network. So, A does not receive any packet coming through B and does not forward to it. Moreover, B will never rejoin the network as seen by node A.

The previous approaches show possible single responses that can be taken by a single node. However, by the assumption of nodes cooperation, these approaches can extend to more than one node or possibly to the whole network by the propagation of second hand information or some sort of alarms.

With these three components of our framework, the following block diagram in figure 1 illustrates our reputation system operation and inter-components relationships.

3.2. Customized reputation system – SNARE overview

This section describes our new customized reputation system that fits into the general framework described earlier. We called our system: ***S**ensor **N**ode **A**ttached **R**eputation **E**valuator* (SNARE) system[82][83].

SNARE is a collection of protocols and algorithms that interacts directly with the network layer. The system consists of three main components; i.e. monitoring component, rating component and response component.

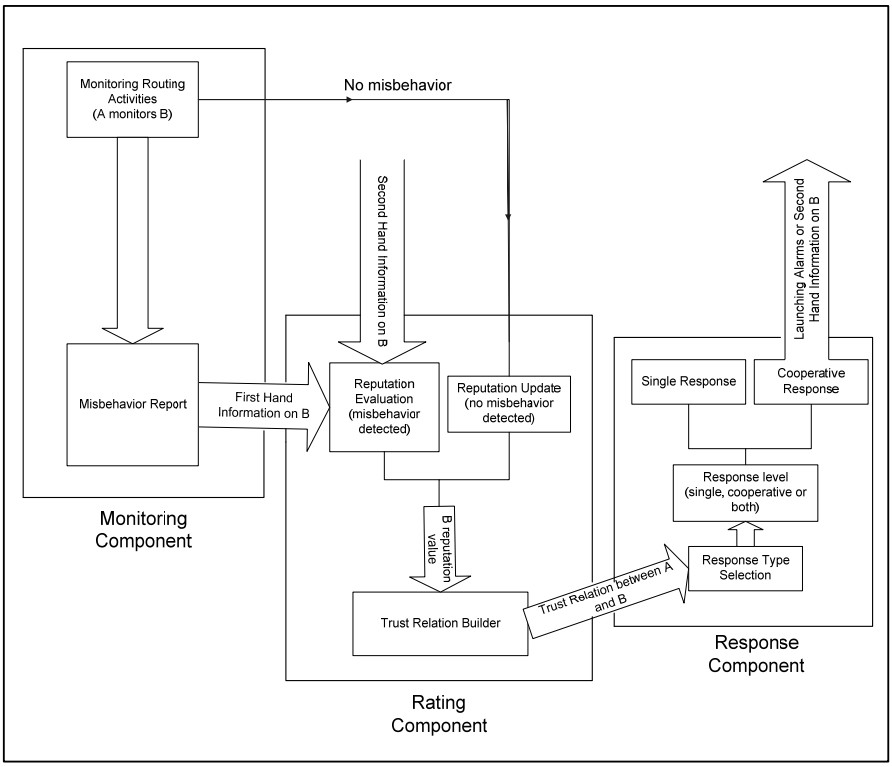

Figure 1. SNARE Reputation system framework

The monitoring component, EMPIRE(Efficient Monitoring Procedure In REputation system)[84], observes packet forwarding events. A monitoring node will not be in a continuous monitoring mode of operation, rather, it will monitor the neighborhood periodically and probabilistically to save resources. When a misbehaving event is detected, it is counted and stored until an update time, T_{update} or T_{ON} is due, then a report is sent to the rating component.

The rating component, CRATER(Cautious Rating for Trust Enabled Routing)[85], evaluates the amount of risk an observed node would provide for routing operation. The risk value is a quantity that represents the previous misbehaving activities that a malicious node (a node that drops packet) obtained. This value is used as an expectation for how much risk would be suffered by selecting that malicious node as a router. It is calculated based on the first hand information and the second hand information. The first hand information is achieved by the direct observation done by the node of concern. Risk values are updated based on the first hand information every time a new misbehavior report is received from the monitoring component. Moreover, if an observed node shows an idle behavior during a certain period, its risk value is reduced. A monitor also updates the risk values of its neighbors by second hand information received periodically from some announcers.

In this work, our system adopts the defensive response approach of the proposed framework. Thus, depending on the trust relations, a node will try to avoid malicious nodes based on the routing decision made by the developed routing protocol - Geographic, Energy, Trust Aware Routing protocol (GETAR). GETAR incorporates the trust information along with distance and energy information to choose the best next hop for the routing operation. The detailed description of this enhanced protocol GETAR is presented in section 4.

3.3. System assumptions

In order to understand how our system works and how simulations have been carried out, it is essential to formally identify the general assumptions on system requirements and boundaries. We will look at system assumptions from different perspectives.

3.3.1. WSN Perspective

In this work, we consider a WSN with a total number of nodes deployed in a random topology or in a grid topology inside a square area. It is assumed that the nodes communicate via bidirectional links so that the nodes can monitor packet forwarding. Moreover, all nodes have equivalent power transmission capabilities, i.e. all have equivalent transmission range. It is also assumed that the consumed power during the simulation time does not impact the transmission range of nodes. This assumption is made to keep the focus of our work on security issues and not on power control. The transmission and reception power are set to 1 Watt whereas the processing power is considered to be 1 milli-Watt per transmission, reception or monitoring operation. Finally, in this work, we assume a static WSN. Mobile WSN can be an interesting subject of a future research work.

3.3.2. Communication model perspective

The system adopts a general communication model in which each node in the system can initiate a routing operation. Thus, any node can be a source. Moreover, any node can be a destination for that node. The selection of the source-destination pair is done randomly. The reason of adopting this model is to study a very general case and not limiting our scope to particular scenarios. Other more realistic scenarios are important to consider. However, such scenarios should also account for the application specifications.

3.3.3. Security perspective

The existence of the reputation system does not imply a complete solution for all security problems. Our proposed solution tries to solve a particular security problem that is related to nodal behavior in the routing operation, as has been discussed earlier. Thus, some reasonable assumptions are made to make the work more focused on our problem:

- The system assumes always-suspicious nodes. This means that a node can not be fully trusted. Every node is assumed to have a minimum risk that can be encountered if that node is used as a router.
- The system assumes a crypto system for any setup requirements. This system is dependent on the routing protocol and, hence, it would imply different implementations that are left to the desire of the operator.
- The system assumes collusion-free attacks. The design of the system, however, can be easily modified to handle collusion based attacks since we adopt modular design. Changes need to be done in the rating component.
- The system treats only one type of behavior related attacks, i.e. non forwarding attack. Although the reputation system can be applied to any other attack, we concentrate here on non-forwarding attack. This is because we are not interested in Intrusion detection Systems (IDS), and we want to maintain the focus of the work on reputation system evaluation.
- The system assumes honesty in treating information exchange about nodes energy levels or risk values. Honesty can be accounted for in the rating component.

3.4. Monitoring component: Efficient monitoring procedure in reputation systems (EMPIRE)

In the context of reputation systems, monitoring is the function that is responsible for observing the activities of the nodes of its interest set, for example, the set of its neighbors.

Monitoring operation can be considered as the most expensive part in terms of resource usage for WSN. That is because it requires a node to track the events occurring around it by overhearing packet transmissions, which consumes lots of energy. Moreover, the computations and allocations of such events may consume a considerable amount of processing power and memory space, which are also important to conserve in WSN. As a result, a node has to monitor the behavior of its neighbors in an efficient manner that can provide a better possible way of resource conservation, while being able to reach to a good conclusion about the neighbors' behaviors so that it will take a proper action based on what it has observed. Thus, an efficient monitoring mechanism should guarantee a satisfactory level of capturing neighborhood activities, while trying to minimize power consumption, memory usage, processing activities, communication overhead, etc.

A new monitoring strategy that is called ***E**fficient **M**onitoring **P**rocedure **I**n **RE**putation system* (EMPIRE) to solve the problem of efficient monitoring in WSN is proposed in [84]. Monitoring efficiency is realized here by the association between the nodal monitoring activity (NMA) and various performance measures. NMA is determined by the frequency of monitoring actions that a node takes to collect direct observation information. Reducing the frequency of monitoring, i.e. reducing NMA, will affect the quantity and/or the quality of the obtained information. Thus, the performance measures will be affected. However, on the other hand, this reduction implies a saving in node's resources such as power, processing and memory. EMPIRE provides a probabilistic approach to reduce nodal monitoring

activities (NMA), while keeping the performance of the system, from the behavior and trust awareness perspective, at a desirable level.

In this procedure as depicted in figure 2, every sensor node is alternating between two nodal monitoring activity states, i.e. ON state and OFF state. A node that is in ON state is a node that performs monitoring activities such as overhearing packets, checking the headers for validation, storing packets to validate events, etc. On the other hand, an OFF node is a node that does not do any monitoring activity. Notice that ON and OFF states are associated with the nodal monitoring activity. Thus, an OFF node may still receive, send and process data not related to monitoring issues. As explained earlier, the objectives of this procedure are realized through the frequency of nodal monitoring activity, NMA. Since nodes alternate between ON and OFF states, reducing NMA is determined by how much a node will stay in each of these states. Thus, when a node stays longer in ON state, its NMA will increase and when it stays longer in OFF state, NMA will decrease. The basic phenomenon of EMPIRE is to allow each node to enter a certain state probabilistically, stay there for a deterministic duration and then, at the end of that duration, it probabilistically leaves its state to the other one or stay for another epoch.

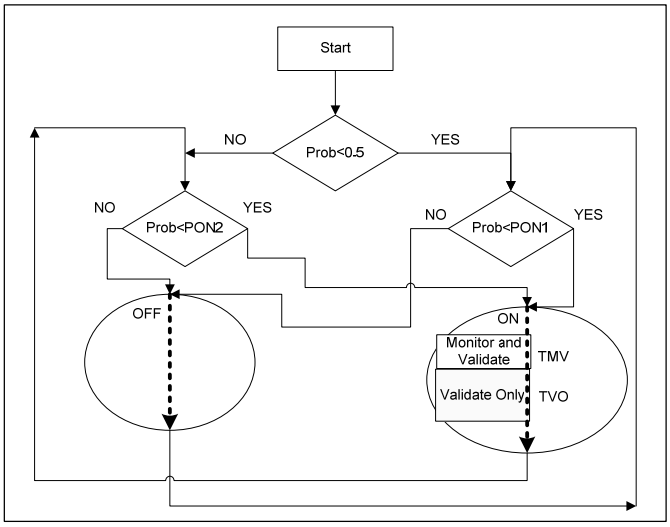

Figure 2. EMPIRE algorithm block diagram

In a cooperative monitoring environment, a node does not need to have a high NMA by continuously monitoring its neighbors' activities as long as there are a sufficient set of nodes that can monitor the same activities. So, if an activity can be monitored by two or more nodes who can share their knowledge among each other, then it is enough to have only one monitor active at a time. Then, upon some scheduling approach, the active node sleeps and another one gets awake. However, this scheduling problem is very complex and depends on different conditions like the network topology, network deployment, nodes mobility, etc.

Thus, in our EMPIRE solution, we are trying to induce a condition-independent and probabilistic "virtual scheduling" among nodes to overcome that problem. It is very important here to emphasize the node cooperation assumption. Node cooperation implies that a node will be willing to inform other nodes about its findings from its NMA. This is known as indirect reputation knowledge sharing or second hand information propagation. With this assumption, nodes will still be able to capture the events it loses during its OFF state. EMPIRE is based on a distributed and probabilistic monitoring approach. The main goal of EMPIRE is to provide good monitoring operation that satisfies the security requirements, while using the least possible nodal monitoring activity. This way, a node will also be able to conserve its resources. Our simulation results show that EMPIRE can satisfy various levels of monitoring requirements with different possible choices of nodal monitoring activity levels. Moreover, EMPIRE is safe in the sense that it can differentiate between malicious and non malicious nodes regardless of the choice of the nodal monitoring activity.

A detailed discussion and analysis of the EMPIRE procedure, simulation setup, performance measures, and simulation results can be found in [84].

3.5. Rating component: Cautious rating for trust enabled routing (CRATER)

In this section, a new rating approach for reputation systems in WSN called CRATER[85] is presented. CRATER evaluates nodes reputation by a risk representation. This risk value is computed based on FHI, SHI and idle behavior (NBP). The mathematical modeling of CRATER assumes a set of conditions that we define as cautious assumptions in which a node is very cautious in dealing with other's information.

In reputation systems, after a node gathers some information regarding the behavior of other nodes of interest, it needs to evaluate or rate these nodes. This is done by the rating function or the rating component of the system. Rating function is based on the node's own observation, other nodes' observations that are exchanged among themselves and the history of the observed node.

The rating component of a reputation system is a very critical part since it is responsible for providing the reputation of nodes. Thus, it can be considered as the heart of any reputation system.

To illustrate the rating operation, assume that node A wants to evaluate a reputation value for a node B that may or may not be directly monitored by A. Then, the reputation value of B evaluated by A is a number that reflects how good or bad node B behaves from the perspective of node A, considering:

- Monitoring results of all types of routing activities.
- Monitoring results obtained by direct observations from A as first hand information, FHI.
- Monitoring results gathered from other nodes observing B and shared with A as second hand information, SHI.

Once a reputation value for B is formed by A, A will decide about a certain level of trust relationship with B

An important issue in rating is the reputation update. Since rating is related to node behavior, the reputation of a node should be a dynamic metric that changes with time. This change would be due to new FHI observations, new SHI, or other defined aspects like, for example, to "forgive" some idle malicious nodes.

A new rating technique called ***C****autious* ***RA****ting for* ***T****rust* ***E****nabled* ***R****outing* (CRATER) is presented in [85]. Basically, this technique identifies three rating factors: FHI, SHI and Neutral Behavior period (NBP) during which a node is not doing any activity. The new contribution in CRATER is its mathematical approach that is used to rate nodes based on what we call cautious assumptions, which are very true in many applications in WSN.

3.5.1. Cautious assumptions

The rating methodology proposed in CRATER assumes what we call "the cautious assumptions". These assumptions are:

- Pessimistic start: The default status of a node joining the WSN network is to be untrustworthy. However, its reputation, or what we will call later the risk value, will not be at the extreme level.
- Unreliable SHI: A node tries to be as much independent from SHI as possible to avoid dishonesty issues.
- Rejecting good news: Announcing "good news" about other nodes in SHI can be a trial from the announcer to relieve itself from routing duties and put the burden on the others or it can be thought as collusion between the announcer and an attacker. Thus, nodes are not interested in hearing good news. On the other hand, "bad news" is very much welcomed. The differentiations between these good or bad announcements are realized by a threshold.
- Local interest: This means that a node is only interested in rating its immediate neighbors.

3.5.2. Rating factors in CRATER

In CREATER, each node rates its neighbor by assigning a risk value to the corresponding monitored node. The risk value of node j assigned by node i, $r_{i,j}$ is defined as a quantity that represents how much risk the node i will encounter when it uses node j as a next hop to route its packets. This value ranges from 0 to 1 where 0 represents the minimum risk and 1 represents the maximum risk. The reputation of node j as per node i is then computed as:

$$rep_{i,j}=1-r_{i,j} \quad (1)$$

The CRATER operation is based on rating the nodes on the risk notion. Each node evaluates the risk values of its neighbors and takes the proper action based on the values it obtains. The risk values are affected by three factors:

- FHI: The direct observation of the neighbor's behavior, this will be referred to as first hand information, FHI.
- SHI: The opinion of other nodes regarding the neighbor of concern. This will be called second hand information, SHI.
- Neutral Behavior Periods (NBP): these are the periods during which a neighbor is observed doing nothing. That is, a neighbor does not receive anything to be tested for forwarding.

Each node in the system continuously and periodically updates the risk values of its neighbors based on the information collected during these update periods .

The general algorithm that a node i follows to rate its neighbor j is:

- Node i monitors node j for the duration of the update period, T_{update}.
- At the end of each update period, do the following:
  - Calculate $r_{i,j,FHI}$ using the new FHI.
  - Update the old risk value, $r_{i,j,old}$ using the new calculated $r_{i,j,FHI}$ to get $r_{i,j}$.
  - Calculate the $r_{i,j,SHI}$ using the SHI.
  - Update $r_{i,j}$ using the $r_{i,j,SHI}$
  - Update $r_{i,j}$ if neutral behavior periods are realized.

When node j is observed by i for n consecutive update periods to be idle in its behavior, node i will give node j a chance to be more trusted by reducing its current risk value. A node is considered to be in idle behavior if it does not perform any routing operation. The reduction procedure follows exactly the same methodology explained in rating based on FHI when $r_{i,j,FHI}=0$. The only difference here is that in the case of neutral behavior the update is done after we observe such behavior during n consecutive update periods whereas it is done immediately after an update period in the case of $r_{i,j,FHI}=0$. The choice of n is a design parameter that depends on how much a network is tolerable against attacks. High values of n mean that we are not willing to forgive malicious nodes quickly.

A detailed discussion and analysis of the CRATER approach, simulation setup, performance measures, and simulation results, can be found in [85].

3.6. Reputation systems-independent scale for trust on routing (RESISTOR)

Reputation systems are very complicated systems to evaluate or compare. This is because each system has its own components' implementation methods, like monitoring strategy, rating approach and response mechanism. All these components affect the efficiency of the reputation system individually as well as a complete system. Therefore, it is important to come up with a simple mechanism that can evaluate and analyze a reputation system. Such a mechanism must be:

- Independent of the reputation system: This means that the inputs of the formulae or equations used in this mechanism should not use the specific parameters that determine how the individual component of the reputation system is working.

- Representative for the effect of each individual component: This means that the mechanism should provide parameters that reflect the role of individual components in the reputation system.

In this work, we propose a simple but strong, independent and representative scale to evaluate reputation systems called ***RE****putaion* ***S****ystems-****I****ndependent* ***S****cale for* ***T****rust* ***O****n* ***R****outing* (RESISTOR)[85].

3.6.1. The resistance concept

RESISTOR is an evaluation procedure that is used to evaluate the performance of reputation systems that are designed to provide trust aware routing. The basic idea behind RESISTOR is to utilize some of the objectives of a reputation system in an analytical way to evaluate the performance of the system.

Any reputation system that is concerned with trustworthy routing has two main objectives:

- Recognizing the malicious nodes by ultimately reaching to their theoretical reputation values or risk values as in the context of CRATER.
- Reducing the flow of packets into the malicious nodes so that they will not have a chance to drop packets, or do any other type of attacks.

Having these two objectives, we introduce the resistance metric. We define, generally, the resistance between node i and a malicious node j in the direction from i to j; $RES_{i,j}$, as a ratio of the risk value $r_{i,j}$ to the number of packets that flow from node i to j, i.e. $P_{i,j}$.

Please notice here that the concept of resistance is only associated with malicious nodes. Thus, if $r_{i,j}$ is high, the resistance value will be high, reflecting that the reputation system is performing well since we are "resisting" a malicious node. Similarly, if $P_{i,j}$ is small, the resistance value gets high, inferring that the reputation system is performing well, too. This is because we expect to pass few packets to a malicious node, ideally zero packets.

The resistance concept is analogous to the resistance phenomenon in electric circuits. We can think of the risk value of a malicious node j as seen by i as the voltage difference between j and i and the packet flow from i to j as the current flow. The resistance, then, increases as the voltage, $r_{i,j}$ increases and the current $P_{i,j}$ decreases similar to Ohm's law; R=V/I. Following this analogy, we have:

$$RES_{i,j} = \frac{r_{i,j}}{P_{i,j}} \tag{2}$$

Thus, a good reputation system must provide high resistance. A perfect reputation system should provide an infinite resistance since $P_{i,j}$=0. A detailed discussion and evaluation of CRATER using RESISTOR approach, simulation setup, and simulation results, can be found in [85].

4. Response component : Geographic, energy and trust aware routing (GETAR) protocol

In this section, an enhanced routing protocol that aims to provide a secure packet delivery service guarantee by incorporating the trust awareness concept into the routing decision is presented. Our proposed protocol is called Geographic, Energy and Trust Aware Routing (GETAR) which is an enhanced version of the Geographic and Energy Aware Routing (GEAR) protocol [9]. GEAR is basically a geographic routing protocol in which the next hop is selected based on two metrics: the distance between the next hop and the destination and the remaining energy level the next hop owns. The new contribution in GETAR is to add a third metric in the next-hop selection process, i.e. the risk value of a node that is computed by the rating component, CRATER in our case.

After a node monitors its neighborhood using EMPIRE and rate them based on CRATER, the node should make the proper response that leads to a proper routing decision. Assume that node A computed a risk value for a malicious neighboring node, B. Then, node A may or may not respond to B's behavior. Since our system treats the secure routing purpose, A should respond in a proper manner. Among different possible reactions provided in many reputation systems [3, 5, 72], we can identify three main response approaches:

- *Defensive approach*: Here, node A just avoids using node B as a router. This avoidance can be gradual as the risk value of node B increases. However, B can still use A or any node to forward its packets.
- *Offensive approach*: In this approach, node A avoids B as in the previous approach. In addition to that, A takes further actions by punishing node B. However, node B still has the right to defend itself and to be treated normally if it can prove a good behavior.
- *Dismissal approach*: In this approach, node A totally ignores node B as if it is not in the network. So, A does not receive any packet coming through B and does not forward to it. Moreover, B will never rejoin the network as seen by node A.

In this work, the defensive approach where malicious nodes are simply avoided without any further actions against them is adopted.

4.1. The original protocol: GEAR

4.1.1. GEAR description

Geographic and Energy Aware Routing [9] (GEAR) is a geographic routing protocol in which the routing decision accounts for the geographic location of a selected node with respect to the destination. It is also considered as a location based routing protocol because nodes are assumed to be interested in communicating with other nodes that reside in certain geographic locations regardless of their identities. The protocol implements greedy forwarding approach based on distance to destination and energy consumption considerations. In fact, the protocol tries to fairly consider energy balancing among the neighbors of a packet forwarder node.

In GEAR, the routing mechanism involves two phases:

- Forwarding the packet to a target region R with a greedy algorithm that tries to balance energy.
- Disseminating the packet within the target region by recursive forwarding.

Forwarding: Forwarding operation in GEAR can be summarized by the following steps:

- Each node N maintains a state value h(N,R) which is called the *learned cost* to region R. A node infrequently updates its h(N,R) value to its neighbors. Thus, every node N has state value knowledge for each neighbor N_i.
- A Source N picks a neighbor N_{min} with the minimum learned value to the region R.
- If N does not have the learned cost of a neighbor N_i, N estimates the learned cost by using the *estimated cost* function $c(N_i,R)$. The function combines the distance d from N_i to R and the consumed energy value e at N_i, as follows:

$$h(N_i,R) \approx c(N_i, R) = \alpha\ d\ (N_i, R) + (1- \alpha)\ e\ (N_i) \quad (3)$$

  where $d(N_i, R)$ is the distance from Ni to the center of R normalized (divided) by the largest such distances among all other candidates. $e(N_i)$ is the so far consumed energy at node N_i normalized by the largest consumed energy among all candidates. α is a tunable weight parameter that varies from 0 to 1 and indicates the routing decision preference. So, if α is close to one, the decision will be biased by the distance. If α is close to zero, the decision will be biased by the consumed energy levels.
- After selecting the N_{min} for routing, N updates its learned cost value to the destination region R as follows:

$$h(N, R) = h\ (N_{min}, R) + c(N, N_{min}) \quad (4)$$

  where the latter term is the cost of transmitting a packet from N to N_{min} considering the same approach in equation (3).

As we can see, from equation (3), when all nodes are equal in energy, the routing decision will be simply the greedy approach as in GPSR [8]. In case all nodes are equidistance from the destination, the selected node will be the one that consumed the least energy among others. This guarantees a fair selection of the node in terms of energy balancing.

Dissemination: Once a packet reaches the center node C_i of the destination region R, the protocol switches to the dessimination phase as follows:

- C_i splits the region R to sub regions R_i, for example four sub regions.
- C_i, then, sends four copies of the packet to the centroids of each sub region R_i.
- Each center node in different sub regions repeats the operation of splitting and forwarding until the center node finds that it is the only node in its sub region.

In our proposed protocol, this phase is avoided and we restrict the operation to forwarding with the cost functions since there is actually no routing decision to be made in the dissemination phase as suggested by GEAR.

Void Regions Problem : If a node wants to forward a packet and it finds out that the learned costs of all its neighbors are greater than its own learned cost, the node should select itself. However, the node's transmission range does not cover the destination. In this case the node is said to be in a void region. GEAR escapes this void region as follows:

- Assume that a source node S wants to transmit a packet to a destination T.
- S selects a next hop, C, that is in a void region, i.e. $h(C,T) < h(N_i,T)$ where N_i is a neighbor to C.
- C forwards the packet to a node, call it B, based on a predefined ordering, e.g. node ID. Then it updates its cost function h(C,T) to be h(C,T)=h(B,T)+c(C,B).
- Now, h(C,R) > h(B,R)
- Later, when node S wants to transmit a new packet to T, it will forward it to B instead of C (see the figure 3).

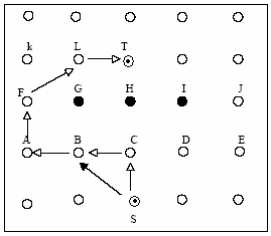

Figure 3. Escaping void regions in GEAR

4.2. The enhanced protocol: GETAR

4.2.1. Basic idea

GETAR is a geographic and energy aware routing protocol that has the additional feature of trust awareness. The trust awareness is achieved by the rating functionality of a running reputation system that will feed the routing protocol with the trust metric that will be the risk values, $r_{i,j}$. The risk value $r_{i,j}$, as discussed earlier, is a quantity that reflects, to some extent, the expectation that a node j will not forward the packet received from node i, assuming non forwarding attack.

The risk value metric, along with distance and energy metrics, are used to compute the learned cost function for each neighbor. The concerned node, then, makes the routing decision by selecting the neighbor of lower cost as in normal GEAR.

As we can see, GETAR is a modification extension to the GEAR protocol to account for some security issues. In GEAR, the choice of a next hop router to the desired destination is made locally by each node based on the learned cost function obtained using equations (3) and (4).

It should be clear that the main idea behind this cost function in GEAR is to provide a tunable preference to the distance or energy consumption as routing metrics based on the value of α. It is important to notice that the two metrics are considered to be routing resources for the node as well as the network. The new contribution in GETAR is to add in

the cost function the risk value as the trust metric to account for trust awareness and which is also considered to be a routing resource.

To illustrate the idea, let's make an analogy between energy and trust. From the energy perspective, a node will prefer to select the next hop that has the least consumed energy level according to GEAR. This local decision and selection is the best effort that the node can do to cooperate in the routing operation and simultaneously conserve the total network energy. Similarly, from the security perspective, a node will prefer to select the next hop that is least risky among others in neighborhood. Such a selection will guarantee the safest decision that the node can do to cooperate in packet delivery. However, the node here tries to maintain trust as a resource.

4.2.2. Forwarding in GETAR

GETAR forwards the packets and makes routing decision following the same procedure in GEAR. However, the major difference is in calculating the estimated cost function that is used to learn the cost to different destinations. In GETAR, the estimated cost function that a node i evaluates for every neighbor j is given by:

$$t(j,R) = \beta r(j) + (1-\beta)[c(j,R)] \tag{5}$$

where t(j,R) is the *trust-aware* cost of using the node j by node i as a router to the center of R. r(j) is the *risk function* that evaluates the risk value of using j as a router. β is a tunable parameter to prefer trust as opposed to other resources.

Using equation (3), we can rewrite equation (5) as:

$$t(j,R) = \beta r(j) + (1-\beta)[\alpha d(j,R) + (1-\alpha)e(j)] \tag{6}$$

If we are concerned about trust more than other resources, β should be close to 1. When β equals 1, the trust-aware cost will consider only the trust part of equation (6) and the next hop will be the most trusted one. Setting β to zero, however, turns the protocol to pure GEAR without any security considerations from the routing protocol perspective.

4.2.3. The risk function r(.)

There can be several ways to represent the risk function evaluated by a node i for using node j as a router. In this work, however, the risk function r(.) is nothing but the risk value $r_{i,j}$. Thus equation (6) is rewritten as:

$$t(j,R) = \beta(r_{i,j}) + (1-\beta)[\alpha d(j,R) + (1-\alpha)e(j)] \tag{7}$$

4.2.4. Dissemination and voids in GETAR

In GETAR, the routing operation involves only packet forwarding phase and does not implement dissemination. This is because in the dissemination phase in GEAR, the packets

are intended to be forwarded to all nodes in the target region. However, when we consider trust awareness, a misbehaving node should not be given a chance to have the packet since it will not forward the packet. Thus, GETAR continues to forward packets based on the routing decisions made by the learned cost function.

Regarding the problem of void regions, there is no change in the escaping operation proposed by GEAR. The only difference in GETAR is that the reason of being in a void region can be also related to the existence of misbehaving nodes in the proximity of the node of interest.

4.3. Simulation objectives and setup

4.3.1. Objectives

In this work, we are studying the effect of incorporating trust aware metric in routing decision in GETAR. The simulation work aims to analyze the following issues:

- The efficiency of GETAR in terms of packet delivery. Therefore, we are analyzing how our proposed protocol will improve the packet delivery, decrease the impact of attacks on dropping packets and decrease the number of packet retransmission due to malicious dropping.
- The efficiency of GETAR in terms of energy conserving. This issue is related to the hypothesis that GETAR will reduce the retransmission due to malicious behavior. Thus, we expect that the power that could have been used for retransmission will be saved with GETAR.
- Studying the impact of malicious nodes population on GETAR performance.
- The trade-off between trust awareness and energy balancing.

4.3.2. Assumptions

- As mentioned earlier in this section, the risk value of a node is assumed to be abstractly calculated by the monitoring and rating components of a reputation system. This risk value is assumed to be constant during the simulation duration. This assumption is valid if we consider that the update period of the risk values is greater than the simulation time, or the updated values during the simulation time are not very far from the starting values. This is valid as long as we assume that the rating and monitoring component have a moderate or slow pace. Moreover, our focus in this work is to study the impact of injecting trust into the routing decision during a period that holds this trust metric unchanged.
- We assume that all nodes are able to locate themselves in the (x,y) coordinates and that sender nodes are able to locate their destinations.
- We assume that nodes will announce their energy and location information honestly. Handling false updates is beyond the focus of this work.
- Attackers are assumed to follow GETAR protocol. They are also allowed to initiate packet transmission sessions. This is because this work does not consider an offensive-

response to malicious behavior. A future work would include that issue, i.e. how to punish malicious nodes from the routing perspective.

4.3.3. Simulation setup

In this simulation work, we used the parameters in table 1. In our simulation, we tested one type of attacks; i.e. non forwarding attack. Moreover, a malicious node in this attack will drop all packets that it receives with probability=1. For this type of attacks, we experiment four different percentages of attackers of the total number of nodes; i.e. 10%, 30%, 50% and 70%.

All experiments are performed by varying the value of the trust awareness parameter β in GETAR cost function. Then, the outputs are used to compare the behavior of the performance metric versus the change in β values.

Parameter	Value	Parameter	Value
Number of nodes	100 nodes	Queuing model	M/M/1
Network dimensions	square 90 units * 90 units	Simulation platform	Event driven simulation using Java programming language
Transmission range	15 units	Simulation duration	100 seconds
Network Deployment	Random topology	Retransmission Timeout	Explicit retransmission request
Power consumption	1 unit per reception and 1 unit per sending operation	Retransmission trials	Unlimited
Mean arrival rate	1 pps	Update Strategy	Periodic, every 5 seconds.
Mean service rate	500 pps	α	0.5 (GEAR parameter)
Outsider attackers deployment	Random	Communication discipline	random source to random destination.
Escaping void	using GEAR part and then distance	Void failure: max number of hops	100

Table 1. Simulation parameters fo GETAR experiments

4.3.4. Performance Measures

- Delivery ratio: This is defined as the ratio between the number of packets delivered successfully to their destinations to the total number of generated packets; i.e:

$$\text{delivery ratio} = \frac{\text{number of successful packets}}{\text{total number of packets}} \tag{8}$$

The objective of this metric is to show the effect of injecting the trust knowledge into the routing decision on improving the success of the routing operation. The metric is studied under the effect of increasing the trust awareness feature by increasing the β parameter of GETAR.

- Outsider attacks' drop ratio: This is defined as the ratio between the number of packets dropped due to outsider malicious nodes to the total number of generated packets; i.e:

$$\text{Outsider attacks drop ratio} = \frac{\text{number of dropped packets by malicious nodes}}{\text{total number of packets}} \tag{9}$$

- Retransmission ratio: This is defined as the ratio between the number of retransmitted packets to the total number of generated packets; i.e

$$\text{retransmit ratio} = \frac{\text{number of retransmissions}}{\text{total packets}} \tag{10}$$

Retransmitted packets include all possible causes, i.e. outsider drops or congestion drops due to voids or exceeding time out. However, if a decrease in this ratio shows up with an increase in β, this proves that most of these retransmissions are due to attacks. Moreover, this ratio indicates the ratio of power spent for packet retransmission to the total network consumed power. Thus, a decrease in this ratio will indicate a saving in power consumption.

- Coefficient of variation of node consumed power (COV): This metric is obtained by dividing the standard deviation of the consumed power per node by the average consumed power per node. A large value of this metric indicates that there is large variation around the mean value. This can be then viewed as a non balancing effect of energy consumption. Small values of this metric indicate that almost all nodes are consuming an amount of power that is around the mean value. This means that there is a better energy balancing among nodes. The metric is computed mathematically as:

$$\text{COV of consumed power} = \frac{\sigma(\text{consumed power})}{\mu(\text{consumed power})} \tag{11}$$

where σ is the standard deviation and μ is the mean.

4.3.5. Simulation results and analysis

4.3.5.1. Delivery ratio

Figure 4 shows the delivery ratio versus β assuming a non forwarding attack. We simulate different scenarios of percentages of attackers from the total population of nodes. The maximum

percentage of attackers is set to 70% as a very pessimistic case to see how GETAR would work with such extreme unacceptable scenarios. However, the practical cases of less percentages are also presented. For each scenario, we can notice that the delivery ratio increases as β increases until a knee point at which the delivery ratio remains almost unchanged. This agrees with the expectation that higher values of β will make GETAR more trust aware and, hence, the developed routes will include fewer attackers. At around β=0.4, all curves saturate at their corresponding maximum possible delivery ratio. This is an interesting result as it indicates that the effect of β is fully utilized for the trust awareness issues at 0.4. This means that increasing β beyond that value is not efficient in terms of trust-awareness. Moreover, as β increases, it will mask the GEAR part of the cost function. Thus, the minimum β that guarantees the maximum achievable delivery ratio is the best choice from the perspective of trust awareness.

Another point to be noticed in this figure is that when β is equal to zero, the delivery ratio is very low (e.g. 0.34 with 10% attackers), while we should expect values around 0.9 since the attackers should drop 10% of the traffic. The reason of this low delivery ratio can be related to GETAR cost function propagation. When a node selects a malicious node as a router, it may get stuck with this router for several transactions before it switches to another router based on energy and distance information. As a result, such low delivery ratio is expected.

The figure also shows the effect of the percentage of the malicious nodes (attackers) in the network on the delivery ratio. As expected, the more the attacker percentage, the less the delivery ratio is. Moreover, the improvement of the delivery ratio by increasing the value of β becomes more significant as attacker percentage increases. For example, with 10% attackers, the ratio increases from 0.34 at β=0 to 0.85 at β=0.4, whereas it improves from 0.1 at β =0 to 0.3 at β=0.4 with 70% attackers. Thus, with 70% attackers, one may decide to keep β<0.4 to give a preference for normal GEAR operation since the delivery ratio is not improving significantly.

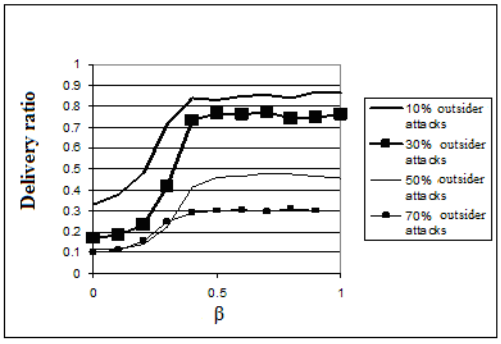

Figure 4. Comparison of the delivery ratio for different attackers' percentage

4.3.5.2. Outsider attacks' drop ratio

Figure 5 provides the relationship between the drop ratio and β parameter. For each scenario of attack percentage, the drop ratio decreases as β increases. The same analysis provided for figure 4 is also valid here.

If we compare this figure with figure 4, we can notice that they almost complement each other. This would be very true if we consider the total drops in the drop ratio to include, in addition to the attack related drops, other drops due to network congestion. However, in our simulation, we are interested only in the attack-related drops. Since this figure is almost complementing figure 4, it is very evident that most of the drops are due to attacks.

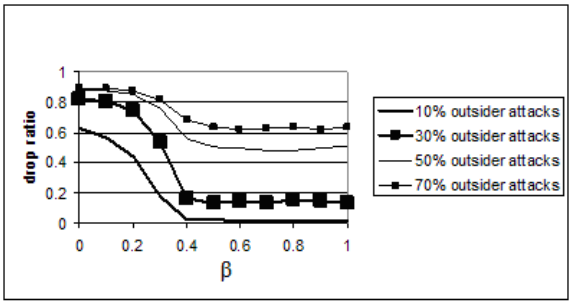

Figure 5. Drop ratio for different attackers percentages

4.3.5.3. Retransmission ratio

The retransmission ratio accounts for two types of retransmitted packets, i.e. packets dropped due to attacks and packets that are not delivered due to path congestion. In figure 6, we can notice two different behaviors of the curves in two regions separated by certain values of β <0.5 for different scenarios. In the first regions for β <0.5, we notice that as β increases, the retransmission ratio increases. This is because when β gets higher values, more packets will suffer longer delays to avoid malicious nodes. Thus, retransmission due to congestion will increase. Also, as we are still below β=0.4, the drops due to attacks are still significant according to figure 5. As a result, an increase in β will cause more retransmissions.

Once we exceed a certain value of β, like 0.4 in case of 30% attackers, most of the packets will have the same routes with the same delays and, as a result, the retransmissions due to congestion will remain almost constant. However, since the drop ratio is decreased dramatically as has been discussed in figure 5, the retransmission ratio will now be affected only by the drop ratio. Thus, the retransmission ratio decreases, also dramatically.

An increase in retransmission ratio gives an indication of the wasted power. That is, the more the retransmission ratio is, the more power is wasted. Thus, an important objective here is to reduce the retransmission ratio as much as possible. However, this fact is very much affected by the percentage of attackers and routing metric preference. For example, assume we have a 10% attackers scenario. It is very obvious that the best choice of β is 0.4 where we have 0 retransmissions or, equivalently, 0 wasted power. However, with 70% attackers, the minimum "wasted power" can be achieved with 0.123 retransmission ratio in two different regions at β <0.3 and β>0.4. In such a situation, if we are more concerned about the energy as a routing metric, it is better to choose β= 0.2 or 0.1. However, if the preference is given for trust awareness, β should be 0.5.

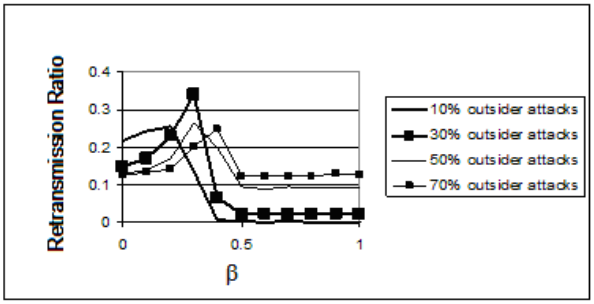

Figure 6. Comparison of the retransmission ratio for different percentages of attackers

4.3.5.4. Coefficient of variation of node consumed power

The importance of the consumed power coefficient of variation metric in figure 7 is to show the impact of trust aware routing decision on energy balancing proposed by normal GEAR. We can see that as β gets higher values, the consumed power coefficient of variation increases until a knee point like β=0.5 in the case of 10% attackers. After that, this metric remains almost unchanged.

Before the knee point, an increase in β will cause the routing decision to select a trusted node with less consideration for energy. This is because high value of β will mask the GEAR part of the cost function. As a result, trusted nodes that are in the proximity of attackers will suffer heavy routing duties whereas other nodes will be balanced with their neighbors. As a result, we will have a larger variation of power consumption as β increases. However, after the knee point, the increase of β will have the same masking effect on the GEAR part of the cost function. Thus, the routing decisions will not change as well.

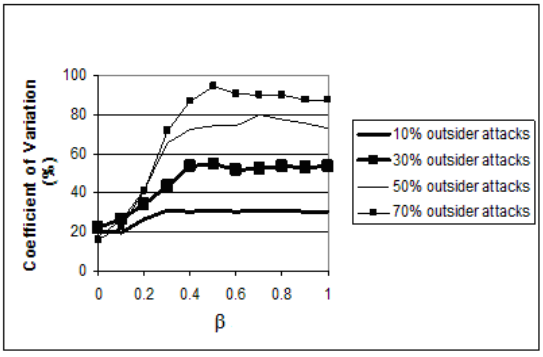

Figure 7. Comparison of the coefficient of variation for different percentages of attackers

This section proposed an enhanced trust aware routing protocol, GETAR, for WSN. The suggested protocol promises to provide trust awareness as well as energy efficiency as it is based on an enhancement of GEAR protocol. This way, GETAR abides by the constrained energy usage in WSN while providing its security service.

5. Comparison with previous work and main contributions

5.1. Routing approach

We provided a simulation based performance analysis for the efficiency of our proposed GETAR routing protocol. Simulation results proved the following points : GETAR improves the delivery ratio, decreases the drop and retransmission ratio and saves the retransmission power when compared with the previous work. The improvement in a performance metric can be achieved at different values of β parameter starting at a minimum value of β at a knee point in the curve. This value can be an optimum choice that guarantees best delivery ratio and better energy balancing. Energy balancing is negatively impacted by an increase in trust awareness. Thus, trade off considerations should be taken carefully in order to design an appropriate value of β. This will be subjected to the application preference between security and energy.

In SAR[70], The routing operation needs to encounter a trusted route setup phase, which contributes some initial delay, especially with the crypto-based authentication required at the route setup. The trust metric used in SAR does not reflect nodes' behavior; rather, they represent a "rank" that a node exhibits based on its identity and various security service provision. Thus, a trusted node in SAR is a node that has the appropriate rank that meets the routing requirements. To rank a node is a problem by itself and requires crypto mechanisms. Our protocol, GETAR, is much simpler in that it assigns trust values to nodes based on nodes behavior. The routing decision rules in SAR are governed by the source, which makes the protocol less flexible. The routing decision is not to select the next hop but to decide to participate in the trusted route. As a result, selfish behavior is not addressed well in SAR. WSN constraints of power consumption are not treated. In fact, SAR targets ad hoc networks with an assumption of more relaxed conditions as compared to WSN.

In TRANS[72], the trust, in fact, is associated with locations rather than nodes. The problem is that a location can be infected by a single node. The detour, then, will be around a larger area rather than a single node. "Innocent" nodes located in proximity of an infected location might be also isolated. If not, they are also exposed to heavy routing duties that may induce selfish behavior. TRANS is limited by single or multiple sink communication models. This assumption is necessary for the efficient operation of the protocol. Our proposed protocol, however, is more generic and can be applied to TRANS model or even for peer-to-peer model. TRANS discusses approaches to decrease energy consumption due to the security provision overhead. However, the protocol does not provide energy efficient techniques in the routing operation itself since it relies on GPSR.

The RGR[73] protocol has no provision for energy efficiency as it relies on GPSR. The protocol totally relies on trust-based forwarding. If a node is completely surrounded by misbehaving nodes, there is no other mechanism proposed to select a next hop since all nodes will be eliminated from the node's forwarding list. RGR is a multi-path trust-based routing. Although multi-path is important for reliable services, we believe that it can be energy consuming which we try to conserve in our work using GETAR.

In RFSN[2], the monitoring mechanism uses a normal watchdog mechanism that assumes a promiscuous mode operation for every node. This is not suitable for the WSN conditions in terms of energy scarcity as discussed earlier. The system does not show a practical solution implementation of monitoring and rating phases. From an implementation point of view, the study should provide an example of how monitoring and rating will be done under some application assumptions. The work does not propose a response methodology, for example, a routing algorithm. Instead, it leaves it as an open issue. Therefore, the work lacks performance figures that can show the efficiency and security gain and benefits in routing operation that can be obtained in adopting this solution.

Main Contributions of our work are the following :

- *Energy awareness*: Our protocol relies on an enhanced operation of GEAR which has energy awareness, whereas RGR, TRANS and SAR do not.
- *Identity-independent trust*: As opposed to SAR and TRANS, our trust metric is behavior-dependent and not identity-dependent. Thus, to obtain trust metrics, we do not require a crypto system to validate nodes identities.
- *Source-sink-Independent routing decision*: In our protocol, routing decision is performed completely based on the individual node vision of the vicinity conditions, whereas in TRANS and SAR, the routing decision is governed by the sink or source requirements.
- *Applicability to different communication models*: Our proposed protocol can be applied to any communication model and architecture

5.2. Rating approach

The rating component of a reputation system deals with combining the first-hand and second-hand information meaningfully into a representative value. Moreover, it is responsible for updating such values as the behavior of nodes are evolving.

In literature, some rating approaches use a single value, called reputation, like CORE [5] and DRBTS [74]. This is similar to our approach in CRATER where we use a single value called the risk value, $r_{i,j}$. Other rating systems like RFSN[2] and CONFIDANT[3] use two separate values, to represent the node reputation.

Some rating approaches updates the node reputation using both first-hand and secondhand information. In CRATER, we use this approach and we also introduce the neutral behavior period as another rating factor. Some other approaches like OCEAN (Observation-based Cooperation Enforcement in Ad Hoc Networks) [75] use just FHI.

In CRATER, SHI is accepted based on the cautious assumptions and the collected SHI by a node i about a node j is averaged to calculate a single $r_{i,j,SHI}$. No validation check or honesty consideration is performed. However, some rating methods use validity and credibility tests for the gathered SHI. One method is to use a deviation test proposed in [64, 74].

Rating functions and mathematical modeling vary depending on the target applications. However, Beta distribution has been the most popular among researchers in reputation and

trust-based systems. It was first introduced in the field by Josang and Ismail [65]. Since then, many researchers have used the beta distribution including Ganeriwal and Srivastava [2] and Buchegger and Boudec [64]. In CRATER, however, we are using a simpler approach similar to the exponential average weighting. This is similar to the approach proposed in DRBTS [74].

When the weighing approach is used, an important issue in maintaining and updating reputation is how past and current information is weighted. For example, CORE tends to give more weight to the past observations assuming that a current observation should have a lower impact on a "greatly built history". On the other hand, RFSN tends to give more weight to recent observations based on the issue of aging. Aging means that we give higher weights to recent observations such that if you behave well you will survive more. As a result, malicious node will be enforced to reduce their attack to survive. In CRATER, we adopt the aging approach with some detailed modifications.

Up to our knowledge, there is no simple and global technique that can independently and efficiently evaluate reputation systems or rating components in the context of WSN and ad hoc networks as compared to our proposed technique, RESISTOR. However, the work in [61] proposes an attempt on comparing reputation systems quantitatively based on game theory. The authors, thus, identify different notions of reputation systems like, contextualization, personalization, individual and group reputation, and, direct and indirect reputation. But, it is more complicated than RESISTOR. Moreover, RESISTOR can be used as an indicator to understand the flaws or plus points in the rating system.

6. Conclusion

The problem of secure routing in WSN is an important area of research that has various aspects of considerations. One important direction under this area is to provide security mechanisms against behavioral related attacks. In this chapter, a comprehensive treatment of the Reputation system based Trust-Enabled Routing framework for wireless sensor networks is provided. We have highlighted the importance of Trust-Aware Routing considering the different network aspects and special conditions of WSN. We have provided a comprehensive review and an in-depth discussion of different Reputation system based Trust-Aware routing approaches highlighting their pros and cons. In our proposed work, we investigated reputation based systems as a promising solution for behavioral related routing security problems. The work developed a new reputation system called SNARE (Sensor Node Attached Reputation Evaluator)[82] that is designed to meet WSN conditions and constraints. This system is divided into three components; i.e. monitoring, rating and response components. Each component is designed with the features that make it possible to apply and then optimize for WSN applications and conditions. In the response component, an enhanced trust aware routing protocol was proposed, called GETAR(Geographic, Energy & Trust Aware Routing). Simulation results showed that this enhanced protocol performs well in terms of increasing packet delivery ratio with tradeoffs in terms of energy balancing. Energy balancing raises an issue of optimization, as well.

As future work, some of the interesting issues to be analyzed to build a robust reputation system are - accurate and efficient trust/reputation modeling and management specific to Wireless Sensor Networks environments, performance of the examined cooperation enforcement with respect to network throughput realized, communication overhead introduced, time required for obtaining accurate reputation ratings/detecting misbehaving nodes, robustness against spurious ratings under a common reference scenario.

Author details

A. R. Naseer
Principal and Professor of Computer Science & Engineering, Jyothishmathi Institute of Technology & Science (JITS), Affiliated to Jawarharlal Nehru Technological University(JNTU) Hyderabad, India

7. References

[1] A. R. Naseer, I.K. Maarouf , and M. Ashraf, "Routing Security in Wireless Sensor Networks", Book Chapter published in Handbook of Research on Wireless Security, Publisher: Idea Group Reference, USA, 2008.
[2] S. Ganeriwal and M. Srivastava, "Reputation-based framework for high integrity sensor networks", Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, pp. 66-77, October 2004.
[3] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes — Fairness In Dynamic Ad-hoc Networks", Proc. IEEE/ACM Symp. Mobile Ad Hoc Net. and Comp., Lausanne, Switzerland, June 2002.
[4] Q. He, D. Wu, and P. Khosla, "SORI: A Secure and Objective Reputation-Based Incentive Scheme for Ad Hoc Networks", WCNC 2004, Atlanta, GA, Mar. 2004.
[5] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks", Commun. and Multimedia Security 2002 Conf. Portoroz, Slovenia, Sept. 26–27 2002.
[6] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. MOBICOM 2000, 2000, pp. 255–65.
[7] Buchegger, S.; Le Boudee, J.-Y, "Self-policing mobile ad hoc networks by reputation systems", Communications Magazine, IEEE Volume 43, Issue 7, July 2005 Page(s):101 – 107.
[8] B. Karp and H. T. Kung. "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", Mobicom 2000.
[9] Y. Yu, R. Govindan, and D. Estrin, "Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks", Technical Report UCLA/CSD-TR-01-0023, May 2001.
[10] Yang Xio, et al. "Security and Routing in wireless Networks", Chapter 4. Nova Science Publishers, Inc. 2005.

[11] Djenouri, D.; Khelladi, L.; Badache, A.N. "A survey of security issues in mobile ad hoc and sensor networks", Communications Surveys & Tutorials, IEEE.Volume 7, Issue 4, Fourth Quarter 2005 Page(s):2 – 28.
[12] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci,"Wireless sensor networks: a survey", Computer Networks 38 (2002) 393–422
[13] A. Cerpa, J. Elson, M. Hamilton, J. Zhao, "Habitat monitoring: application driver for wireless communications technology", ACM SIGCOMM'2000, Costa Rica, April 2001.
[14] C. Jaikaeo, C. Srisathapornphat, C. Shen, "Diagnosis of sensor networks", IEEE International Conference on Communications ICC'01, Helsinki, Finland, June 2001.
[15] B. Warneke, B. Liebowitz, K.S.J.Pister, "Smart dust: communicating with a cubic millimeter computer",IEEE Computer (January2001) 2–9.
[16] http://www.fao.org/sd/EIdirect/EIre0074.htm
[17] J.M. Kahn, R.H. Katz, K.S.J. Pister, "Next century challenges: mobile networking for smart dust", Proceedings of the ACM MobiCom'99, Washington, USA, 1999, pp. 271–278.
[18] N. Noury, T. Herve, V. Rialle, G. Virone, E. Mercier, G. Morey, A. Moro, T. Porcheron, "Monitoring behavior in home using a smart fall sensor", IEEE-EMBS Special Topic Conference on Microtechnologies in Medicine and Biology, October 2000, pp. 607–610.
[19] D. Estrin, R. Govindan, J. Heidemann, "Embedding the Internet", Communication ACM 43 (2000) 38–41.
[20] N. Priyantha, A. Chakraborty, H. Balakrishnan, "The cricket location-support system", Proceedings of ACM MobiCom'00, August 2000, pp. 32–43.
[21] Karl, Holger, Willig, Andreas, "Protocols and architectures for wireless sensor networks", Wiley, c2006.
[22] Slijepcevic, S.; Potkonjak, M.; Tsiatsis, V.; Zimbeck, S.; Srivastava, M.B."On communication security in wireless ad-hoc sensor networks. Enabling Technologies: Infrastructure for Collaborative Enterprises", WET ICE 2002, Proceedings. Eleventh IEEE International Workshops on 10-12 June 2002 Page(s):139 – 144.
[23] Krishnamachari, Bhaskar, "networking wireless sensors", Cambridge University Press, 2005.
[24] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, " SPINS: Security Protocols for Sensor Networks", Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001.
[25] G.J. Pottie, W.J. Kaiser, "Wireless integrated network sensors", Communications of the ACM 43 (5) (2000) 551–558.
[26] J.M. Rabaey, M.J. Ammer, J.L. da Silva Jr., D. Patel, S. Roundy, "PicoRadio supports ad hoc ultra-low power wireless networking", IEEE Computer Magazine (2000) 42–48.
[27] Kemal Akkaya, Mohamed Younis, "A Survey on Routing Protocols for Wireless Sensor Networks", Department of Computer Science and Electrical Engineering. University of Maryland.
[28] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks", Proceedings of the 5th Annual ACM/IEEE

International Conference on Mobile Computing and Networking (MobiCom'99), Seattle, WA, August 1999.

[29] C. Intanagonwiwat, R. Govindan and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00), Boston, MA, August 2000.

[30] D. Braginsky and D. Estrin, "Rumor Routing Algorithm for Sensor Networks", Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA, October 2002.

[31] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless sensor networks", in the Proceeding of the Hawaii International Conference System Sciences, Hawaii, January 2000.

[32] A. Manjeshwar and D. P. Agrawal, "TEEN : A Protocol for Enhanced Efficiency in Wireless Sensor Networks", in the Proceedings of the 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, April 2001.

[33] T. He et al., "SPEED: A stateless protocol for real-time communication in sensor networks", in the Proceedings of International Conference on Distributed Computing Systems, Providence, RI, May 2003.

[34] C. Perkins, "Ad Hoc Networks", Addison-Wesley, Reading, MA, 2000.

[35] Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003.

[36] T. Grandison and M. Sloman, "A survey of trust in internet applications," *IEEE Comm. Surveys & Tutorials*, vol. 3, no. 4, 2000.

[37] S. Marsh, "Formalising Trust as a Computational Concept," in *Departmet of Computer Science and Mathematics*, vol. PhD: University of Stirling, 1994, pp. 184.

[38] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara, "Reputation systems: Facilitating trust in internet interactions," *Comm. of the ACM*, vol. 43, no. 12, pp. 45–48, 2000.

[39] Li H, Singhal M. A Secure routing protocol for wireless ad hoc networks. *39th Hawaii International Conference on system Sciences*, Kauai, 2006.

[40] Rezgui A, Eltoweissy M, TARP: a trust-aware routing protocol for sensor-actuator networks. *IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, Pisa, Italy, 2007.

[41] Hur J, Lee Y, Yoon H, Choi D, Jin S. Trust evaluation model for wireless sensor networks. *Advanced Communication Technology Conference*, Phoenix Park, Korea, 2005; 491–496.

[42] Crosby GV, Pissinou N. Cluster-based reputation and trust for wireless sensor networks. *Consumer Communications and Networking Conference*, Las Vegas, NV, USA, 2007.

[43] Lewis N, Foukia N., Using trust for key distribution and route selection in wireless sensor networks. *IEEE Globecom*, Washington DC, USA, 2007.

[44] Jing, Q.; Tang, L.Y.; Chen, Z. Trust Management in Wireless Sensor Networks. *J. Softw.* **2008**, *19*, 1716-1730.

[45] Hur J, Lee Y, Yoon H, Choi D, Jin S. Trust evaluation model for wireless sensor networks. *Advanced Communication Technology Conference*, Phoenix Park, Korea, 2005; 491–496.

[46] G. Theodorakopoulos and J. S. Baras, "On trust models and trust evaluation metrics for ad hoc networks," *IEEE J. on Selected Areas in Comm.*, vol. 24, no. 2, pp. 318–328, Feb. 2006.

[47] Marmol, F.G.; Perez, G.M. Towards Pre-standardization of Trust and Reputation Models for Distributed and Heterogeneous Systems. *Comput. Stand. Interfaces* **2010**, *32*, 185-196.

[48] G. Shafer, "A mathematical theory of evidence,", Princeton University, 1976.

[49] M. Momani, S. Challa, and K. Aboura, "Modelling Trust in Wireless Sensor Networks from the Sensor Reliability Prospective," presented at International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CIS2E 06) University of Bridgeport, USA, 2006.

[50] M. Momani, K. Aboura and S. Challa, "RBATMWSN: Recursive Bayesian Approach to Trust Management in Wireless Sensor Networks", in *The Third International Conference on Intelligent Sensors, Sensor Networks and Information*, Melbourne, Australia, 2007.

[51] P. A. Morris, "Bayesian expert resolution," in *Department of Engineering-Economic Systems*, vol.Ph.D: Stanford University, 1971.

[52] D. V. Lindley and N. D. Singpurwalla, "Reliability (and fault tree) analysis using expert opinions. ," *Journal of the American Statistical Association*, vol. 81, pp. 87-90, 1986.

[53] Feng, Renjian; Xu, Xiaofeng; Zhou, Xiang; Wan, Jiangwen. 2011. "A Trust Evaluation Algorithm for Wireless Sensor Networks Based on Node Behaviors and D-S Evidence Theory." *Sensors* 11, no. 2: 1345-1360, 2011

[54] Dempster, A. Upper and Lower Probabilities Induced by Multivalued Mapping. *Ann. Math. Stat.* **1967**, *38*, 325-339.

[55] Lopez, J.; Roman, R.; Agudo, I.; Fernandez, C.G. Trust Management Systems for Wireless Sensor Networks: Best Practices. *Comput. Commun.* **2010**, *33*, 1086-1093.

[56] Li, J.L.; Gu, L.Z.; Yang, Y.X. A New Trust Management Model for P2P Networks with Time Self-Decay and Subjective Expect. *J. Electron. Inf. Technol.* **2009**, *31*, 2786-2790.

[57] Li, L.; Fan, L.; Hui, H. Behavior-Driven Role-Based Trust Management. *J. Softw.* **2009**, *20*, 2298-2306

[58] Lewis N, Foukia N., Using trust for key distribution and route selection in wireless sensor networks. *IEEE Globecom*, Washington DC, USA, 2007.

[59] Atakli IM, Hu H, Chen Y, Ku WS, Su Z. Malicious node detection in wireless sensor networks using weighted trust evaluation. *Spring Simulation Multiconference*, Ottawa, Canada, 2008.

[60] http://en.wikipedia.org/wiki/Reputation_systems

[61] L. Mui, A. Halberstadt, and M. Mohtashemi, "Notions of Reputation in Multi-Agents Systems: A Review", *Proc. First Int'l Joint Conf. Autonomous Agents and Multi-Agent Systems*, pp. 280-287, July 2002.

[62] http://www.ebay.com
[63] http://www.epinions.com
[64] S. Buchegger and J.-Y. L. Boudec, "A Robust Reputation System for Mobile Ad-hoc Networks", EPFL IC, Tech. Rep. IC/2003/50, July 2003.
[65] Audun Josang, Roslan Ismail, "The Beta Reputation System", 15th Bled Electronic Commerce Conference, e-Reality: Constructing the e-Economy. Bled, Slovenia, June 2002.
[66] Deng, R. Han, and S. Mishra, "Insens: Intrusion-tolerant Routing in Wireless Sensor Networks", 23rd IEEE Int'l. Conf. Distributed Comp. Sys. (ICDCS 2003), May 2003.
[67] Oniz, C.C. Tasci, S.E. Savas, E. Ercetin, O. Levi, A, "SeFER: secure, flexible and efficient routing protocol for distributed sensor networks", Proceedings of the Second European, Workshop on Wireless Sensor Networks, 2005. Publication Date: 31 Jan.-2 Feb. 2005
[68] S. Buchegger and J.-Y. Le Boudec. A Robust Reputation System for Peer-to-Peer and Mobile Ad-hoc Networks. *Proceedings of P2PEcon 2004*, Harvard University, Cambridge MA, U.S.A., June 2004.
[69] S. Buchegger, C. Tissieres and J.-Y. Le Boudec. A Test-Bed for Misbehavior Detection in Mobile Ad-hoc Networks - How Much Can Watchdogs Really Do?. *Proceedings of IEEE WMCSA 2004*, English Lake District, UK, December 2004.
[70] S. Yi, R Naldurg, and R. Kravets, "Security-aware Ad-hoc Routing for Wireless Networks", ACM Wksp. Mobile Ad Hoc Networks, Mobihoc, 2001.
[71] S. Buchegger and J.-Y. Le Boudec, "A Robust Reputation System for Peer-to-Peer and Mobile Ad Hoc Networks", P2PEcon, Harvard Univ., Cambridge, MA, June 2004.
[72] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Location-centric isolation of misbehavior and trust routing in energy-constrained sensor networks", April 2004.
[73] Nael AbuGhazaleh, Kyoung Don Kang and Ke Liu. "Towards Resilient Geographic Routing in WSNs", MSWiM'05, October 10–13, 2005.
[74] A. Srinivasan, J. Teitelbaum and J. Wu, "DRBTS: Distributed Reputation based Beacon Trust System", 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06), Indianapolis, USA, pp. 277–283, 2006.
[75] S. Bansal and M. Baker, "Observation-based Cooperation Enforcement in Ad Hoc Networks", http://arxiv.org/pdf/cs.NI/0307012, July 2003.
[76] M. Krasniewski, P. Varadharajan, B. Rabeler, S. Bagchi, and Y. Hu, "TIBFIT: Trust Index Based Fault Tolerance for Arbitrary Data Faults in Sensor Networks", Proceedings of the International Conference on Dependable Systems and Networks (DSN'05), (Yokohama, Japan), June 2005.
[77] Z. Yao, D. Kim, and Y. Doh. PLUS: Parameterized and localized trust management scheme for sensor networks security. In *Proc. of the 3rd IEEE Int. Conf. on Mobile Ad-hoc and Sensor Systems*, pages 437–446, Vancouver, Canada, Oct. 2006.
[78] Hu, J., Burmester, M., 2006. "LARS: a locally aware reputation system for mobile ad-hoc networks", in *44th annual ACM Southeast Regional Conference, 2006*.

[79] G. Zhan, W. Shi, and J. Deng, "Tarf: A trust-aware routing framework for wireless sensor networks," in *Proceeding of the 7th European Conference on Wireless Sensor Networks (EWSN'10)*, 2010.

[80] Zhan, G., Shi, W., Deng, J., "Sensortrust - a Resilient trust model for WSNs", SenSys 2009, Proceedings of the 7th International Conference on Embedded Networked Sensor Systems (2009)

[81] M. Momani and S. Challa, "GTRSSN: Gaussian Trust and Reputation System for Sensor Networks", in *International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE '07)*, University of Bridgeport 2007.

[82] I. K. Maarouf and A. R. Naseer, "SNARE : Sensor Node Attached Reputation Evaluator", in Proceedings of IEEE/ACM 2nd International CONEXT conference, Dec. 4-7, 2006, Lisboa, Portugal.

[83] I. K. Maarouf and A. R. Naseer, "WSNodeRater: An optimized Reputation System Framework for Security Aware Energy Efficient Geographic Routing in WSNs", in Proceedings of ACS/IEEE International Conference on Computer Systems and Applications, AICCSA '2007, May 13-16, 2007 Amman, Jordan.

[84] A. R. Naseer, I.K. Maarouf, U. Baroudi, , "Efficient Monitoring Approach for Reputation System based Trust-aware Routing in Wireless Sensor Networks", International Journal of IET Communications – Wireless Adhoc Networks, May 2009, Volume 3, Issue 5, pp. 846-858, ISSN 1751- 8628

[85] I.K. Maarouf, U. Baroudi, A. R. Naseer, "Cautious Rating for Trust-enabled Routing in Wireless Sensor Networks", EURASIP International Journal on Wireless Communications and Networking, 2010, Volume 2, Article ID 718318, 16 pages, ISSN: 1687-1472.