Research Journal of Applied Sciences, Engineering and Technology 9(11): 1016-1026, 2015
DOI:10.19026/rjaset.9.2595
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: December 10, 2014 Accepted: January 27, 2015 Published: April 15, 2015

Research Article

A Survey of Wireless Sensor Network Security and Routing Techniques

Raja Waseem Anwar, Majid Bakhtiari, Anazida Zainal and Kashif Naseer Qureshi
Faculty of Computing, Universiti Teknologi Malaysia, 81310 Skudai, Johor Bahru, Malaysia

Abstract: The main purpose of the study is to review the evolution of wireless sensor network security and routing techniques. Recent years have seen tremendous growth in Wireless Sensor Networks (WSNs). As WSN's become more and more crucial to everyday life, their security and trust become a primary concern. However because of the nature of WSNs, security design can be challenging. Trust-aware routing protocols play a vital role in security of Wireless Sensor Networks (WSNs). The review study provides an overview of Wireless Sensor Network (WSN) and discusses security issues and the routing techniques for high quality of service and efficient performance in a WSN. In order to identify gaps and propose research directions in WSN security and routing techniques, the study surveys the existing body of literature in this area. The main focus is on trust concepts and trust based approaches for wireless sensor networks. The study also highlights the difference between trust and security in the context of WSNs. The trust and security are interchangeable with each other when we elaborate a secure system and not same. Various surveys conducted about trust and reputation systems in ad hoc and sensor networks are studied and compared. Finally we summarize the different trust aware routing schemes.

Keywords: Attacks, blackhole, protocols, security, trust, WSN

INTRODUCTION

Technological advancements in wireless communication technologies have led to the development of inexpensive sensor nodes. The availability of these nodes has made Wireless Sensor Networks (WSN) one of the most promising technologies of the past decade. A wireless sensor network is formed by a large number of distributed sensor nodes in a particular environment for sensing and monitoring. In most cases, these tiny sensors nodes are equipped with an antenna, radio transceiver, a processor, memory and a battery. The function of these independent nodes is monitoring, sensing and collecting data within a specific area and sending this information back to base station for analyzing. The base station acts as a gateway for connecting with end user points. Wireless communication is used to transmit data between sensor nodes and base station using a set of predefined rules called routing protocols (Abd-El-Barr *et al*., 2005). Due to nature of Wireless Sensor Networks, routing in a sensor network is very challenging because of many features that distinguish sensor networks from other wireless networks (Perrig *et al*., 2004; Akkaya and Younis, 2005; Nivetha and Venkatalakshmi, 2012). As compared to wired networks, harsh deployment environment of sensor networks makes them vulnerable to physical and logical security attacks. Various types of routing protocols have been proposed for WSNs however none of them completely secure the sensor nodes (Boukerche *et al*., 2011). A WSN is characterized by its broadcast nature, frequently changing topology, unsupervised manner of operation and transmission medium. These factors make the design of routing protocols very challenging. In presence of these factors routes are easily discontinued. Additionally links between nodes may have limited bandwidth, limited energy and stringent resources (Kohno *et al*., 2012). The secure routing protocols should be lightweight and minimize energy consumption and complexity. One of the main concerns in WSN applications is to design a secure routing protocol that is able to operate in a harsh and unattended environment. Security is one of the most important and useful metric for routing protocols (Nikjoo *et al*., 2007). A secure routing protocol ensures connectivity in the presence of node failure and security attacks.

In this study, we present the evaluation of some popular and well-known wireless senor network routing protocols with their security techniques and study their limitations and strengths in detail.

MATERIALS AND METHODS

Model of wireless sensor network: The wireless sensor network consists of many nodes and every node independently senses and computes in the network. The

Corresponding Author: Raja Waseem Anwar, Faculty of Computing, Universiti Teknologi Malaysia, 81310 Skudai, Johor Bahru, Malaysia

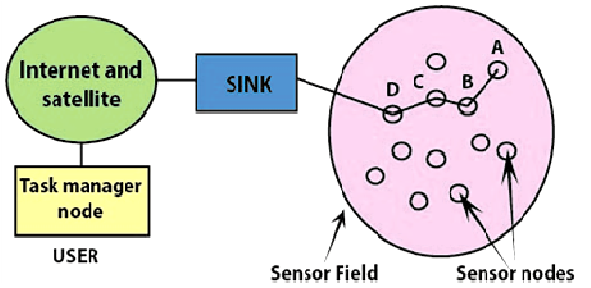

Fig. 1: Wireless sensor network components (Kaplantzis *et al*., 2006)

nodes in network communicate and forward the sense data to a central processing unit. A commonly used sensor node is the Mica2 Mote developed by Crossbow technology. The wireless sensors are deployed densely and with limited resources in a network. The topology of a network is changing constantly and uses broadcast communication medium. The sensors are not based on global identification tags (Sharma *et al*., 2009). The main components of network are sensor field, sensor node, sink node and task manager. The sensor field is an area where all nodes are placed for sensing the information such as ground or a battle field. The sensor nodes are the major components and collect and forward information to other nodes. The sink nodes are called aggregation point because they have a specific task of processing, receiving and storing the data from other nodes. A sink node overcomes the energy requirement and manages the messages. In last task, manager or base station is a centralized part of network for controlling the communication. The base station is usually in the form of a laptop or computer with high processing and storage capabilities. The data is streamed via internet, wireless channels and satellite. Various sensor nodes are deployed in a field to create a wireless multi-hop network. Sensor nodes use wireless communication media such as infrared, radio, optical media or Bluetooth for their communications. Figure 1 shows the components of a sensor network.

Operating systems and applications: An operating system runs reliable application software and provides compatible hardware resources. The wireless sensor network operating systems are typically less complex compare with others OS because the sensor are used for special purpose and the sensor hardware has limited capabilities. The tiny OS was the first operating system specifically designed for WSN. Now a day's many OS are working in WSN nodes such as SOS (SOS embedded Operating System), LiteOS. The applications of sensor networks are valuable and practical in military as well as civilian environments. In Military, the applications can be used for battlefield monitoring, equipment and ammunition, battle damage assessment,

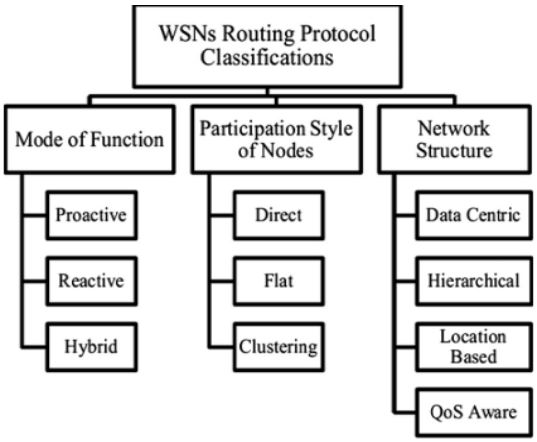

Fig. 2: WSN routing protocol classifications

targeting and reconnaissance applications monitoring. In other fields, they can be used for environmental monitoring purposes and in health applications, building automated, smart environments, such as bridges, robot control and guidance in automatic manufacturing environments, factory process control and automation, vehicle tracking and detection, monitoring disaster areas, increasing the effectiveness of agricultural processes and water management (Akyildiz *et al*., 2002; Buttyan and Hubaux, 2008).

Routing in wireless sensor network: This section elaborates various WSN routing protocols. Routing is a method to send the data over a network between two nodes and routing protocols are used for performing the routing. The protocols select the most efficient path for the data to reach the target node. The network layer is responsible to implement the routing of the incoming data. Most of the source nodes cannot reach to destination due to their transmission range and in this situation; the intermediate sensor nodes forward the packets. As noted before, a WSN has some constraints such as energy supply, bandwidth etc. In past a number of routing protocols have been designed for WSN, such as LEACH, Directed Diffusion, (Heinzelman *et al*., 2000; Intanagonwiwat *et al*., 2000), APTEEN (Manjeshwar and Agrawal, 2001), SPEED (He *et al*., 2003). These protocols mostly focused on energy consumption. The designs of protocols are tailored by application scenario and backbone of network. Based on previous work, this study focuses on secure routing protocols (Fig. 2).

The WSN routing protocols are classified based on mode of functions, network structure and participation styles of sensor nodes. The mode of function protocols can be proactive, reactive or hybrid. In participation mode the protocols could be flat, direct and clustering based. In network structure mode protocols can be data-centric, location based, hierarchical or QoS (Quality of Service) based.

Mode of function based protocols: The first classification of WSN routing protocols is based on mode of function and these modes are proactive, reactive and hybrid (Niezen *et al*., 2007). In proactive protocols, the routing table is generated at every node and the routing information of complete network is periodically updated. Pre-provisioning is also done for all possible paths for the entire network topology. In this approach, the data traffic can be sent out to its destination immediately, without the delay imposed by route acquisition in reactive protocols. However, a certain amount of control traffic is needed to keep routing tables up to date and reliable over the entire network. This control traffic is always present, independent of data traffic on the network.

In reactive routing protocols no routing table is generated and route discovery is done as required. The routes between nodes are attained on demand. The source node triggers a route discovery request through the network and waits for a response from the destination node. Sometime this process takes time and causes a delay in network and overhead control depends on the data traffic in the network. By acquiring routes on demand, a node has only a partial knowledge about the network, as routes are computed only for destinations to which data traffic has to be forwarded. This might be advantageous in terms of state, as reactive protocols do not require each node to store routes for the entire network. The combination of reactive and proactive protocols is called hybrid. The hybrid approach decreases the cost of the network. It first computes all routes and then improves routes at the time of routing.

Participation style of nodes based: The second classification is participation style of nodes and in this category, three types of routing protocols are: direct, flat and clustering present (Pal *et al*., 2010). The direct type is based on sending all information directly to the base station. In flat type the nodes primarily find a valid route to the base station and then forward the packets to sink node or other nodes through routing responsible for collecting and communicating the data with the sink node such as Sensor Protocols for Information via Negotiation (SPIN) (Heinzelman *et al*., 1999), Direct Diffusion (DD) and Rumour Routing (Intanagonwiwat *et al*., 2000; Braginsky and Estrin, 2002). In clustering types the area is divided into number of small clusters. In which cluster head directly communicates with base station.

Network structure based protocols: The third classification is network structure type and in this category the protocols types are: data centric, hierarchical and location-based and QoS aware based (Abd-El-Barr *et al*., 2005). The data centric protocols depend on the tag or naming of the desired data and are responsible for eliminating redundant transmissions. In this category, the target node sends queries requesting certain data from the nodes in the network and if data matches the query, it sends them back to the requesting node. This process is belonging falls under the query based routing approach and is also known as Directed Diffusion. The examples of query based routing protocols are Directed Diffusion (DD), COUGAR (Yao and Gehrke, 2002), Sensor Protocols for Information via Negotiation (SPIN). The hierarchical based protocols perform energy efficient routing and select higher energy nodes for processing and send the information to cluster head while low energy nodes sensing the proximity of the target (Zhan *et al*., 2009). These types of protocols perform energy-efficient routing in WSNs and are best for reducing the amount of overall message transmissions. The most popular routing protocols in this category are Low Energy Adaptive Clustering Hierarchy (LEACH) (Heinzelman *et al*., 2000), Power-Efficient Gathering in Sensor Information Systems (PEGASIS) (Lindsey and Raghavendra, 2002), Threshold-sensitive Energy Efficient sensor Network protocol (TEEN) (Manjeshwar and Agrawal, 2002), Adaptive Periodic TEEN (APTEEN) (Manjeshwar and Agrawal, 2001) and Small Minimum Energy Communication Network (MECN) (Rodoplu and Meng, 1999). The location-based protocols require location information of sensor nodes usually accessed from GPS (Global Positioning System) signals or received radio signal strength. In this category, the routing protocols work on their location for calculating the distance to its neighbor node from the incoming signal strength. To save energy in network the nodes use active or sleep state, in active state the node is alive and in sleep state the node rests if there is no activity. In some location-based schemes in order to save energy, the nodes must change their state between active or sleep. The most popular routing protocols in this category are Geographic Adaptive Fidelity (GAF) (Xu *et al*., 2001) and Geographic and Energy Aware Routing (GEAR) (Yu *et al*., 2001). The Quality of Service (QoS), aware routing focuses on many network layer requirements such as reliability and latency. The sensor network is based on balance function and quality of network, energy efficiency and data quality. In particular, the sensor networks need some quality of service metrics such as delay, energy, bandwidth, for delivering data. The popular protocols that fit in this category are SPEED (Stateless Protocol for Real-Time Communication in Sensor Networks) (He *et al*., 2003) and Sequential Assignment Routing (SAR) (Sohrabi *et al*., 2000) (Fig. 3).

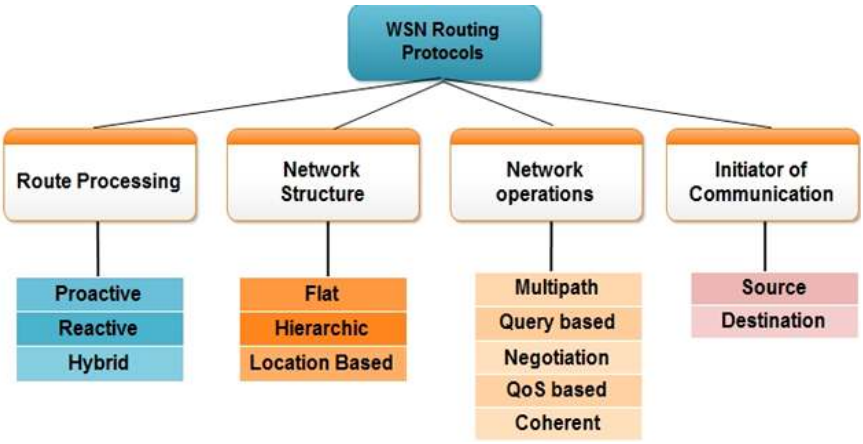

Fig. 3: Classification of WSN routing protocols

Design requirements and challenges: The existing routing protocols employ different strategies for securing routing operations in network. In WSN the nodes run routing protocols in a self-organized manner and have a dynamic topology. This section discusses the detail about design and properties which need to be satisfied to ensure security. Due to the insecure nature of sensor nodes such as ease of deployment, broadcast communication and low cast device, the security requirement is essential to protect the network from potential attackers or intruders.

Security in wireless sensor network: The advancement in wireless sensor networks has proved that they provide various advantages over traditional methods. One of the main challenges is provision of security in the network because of the possibility of the presence of one or more faulty and malicious nodes in the network (Al-Karaki and Kamal, 2004). The sensor node is at risk because of attackers that capture the node secret keys; this is referred to as insider attack (Srinivasan *et al*., 2009). Several security challenges have been discussed in different literature reviews such as Perrig *et al*. (2004), Pathan *et al*. (2006) and Wang *et al*. (2006). In security attack, an adversary node would appear to be a legitimate member of the network. When the node is captured, an adversary may sniff and inject packets with falsified data and may reprogram the sensor node and carry out system faults and bad routing by malicious nodes, which may eventually prove detrimental to the overall system. Because of these attacks, the security is a main issue, which must be addressed for a secure network. There are some external attacks in WSN that are addressed by the use of cryptographic techniques but this technique is not effective against the internal attacks by a malicious node. Nodes do not support the heavy computations of cryptography-based protocols because the nodes are constrained by their limited resources.

Efficient security protocols that are resource economical, capable to provide protection at node-level and meet the security demands of the application are required. Recently the basic ideas of trust and reputation have been applied to WSNs for monitoring changing behaviors of nodes in a network. Reputation and trust are two very useful tools that are used to facilitate decision making in diverse fields from an ancient fish market to state-of-the-art e-commerce (Srinivasan *et al*., 2009).

Trust and security are interchangeable concepts in wireless sensor networks. Security is different from trust because security means no one is trusted and requires authentication all the time and this leads to very high overhead, while, trust means everybody is trusted somehow and does not require authentication (less overhead) (Momani, 2010).

The trust and security based approaches have gained global recognition in WSNs (Khalid *et al*., 2013). Trust Reputation Models (TRM), deals with the problem of uncertainty in decision-making, by keeping the history of a node's previous behavior (repute). A node is trusted and will be forwarded with the packets only if the node holds a good repute; otherwise, the node will be considered untrustworthy. The same concept is applied in Trust Reputation Models (TRMs); a node will prefer to interact with a well-reputed neighboring node.

Security objectives: Security is one of the essential factors in any real time application. In data exchange phase it can greatly affect the whole network. During designing of a WSN the security attributes must be considered. The WSN has unique characteristics like wireless communication medium, resource constrained capability, dynamic topology and these characteristics open WSN for different attacks. The adversaries easily eavesdrop, inject, intercept or alter the transmitted messages. Before deploying WSN the security precautions must be taken into account. The security is important when every source node sends packets to destination nodes. WSNs are prone to different types of

attacks, some important security objectives that must be considered in designing a WSN network include authentication (Sen, 2009), integrity (Burgner and Wahsheh, 2011), confidentiality, availability (Stavrou and Pitsillides, 2010) and freshness (Sen, 2009).

Security attacks in wireless sensor network: In past various type of WSN routing protocols were designed without considering security functionalities (Yahya and Ben-Othman, 2009a, b; Guo and Zhong, 2010), an adversary can set up diverse of attack on the network such as data forgery, Denial-of-service and node capture attacks (Wood and Stankovic, 2002; Perrig *et al*., 2004). Moreover, the security attacks can focus on different goals of sensor network. The basic goal of attackers is to disturb and completely paralyze the routing operation. The node security is a significant need in the network and a malicious node can collapse the whole network at worst, beside the disclosure of some vital network information. The attacks can be classifies in different ways but main categories are passive and active attacks (Deng *et al*., 2002). In passive attacks the information is transmitted by eavesdropping without disrupting the routing protocol operations. The active attacks can be classified into internal and external types. The node misbehaves in many different ways and can become resource deficient. Therefore, we must understand the various types of node misbehaviors that WSNs may usually encounter. There are two common types of misbehaving nodes (Cho *et al*., 2011) selfish and malicious nodes. The selfish node does not cooperate with other nodes because of some resource constraint like low battery. A selfish node may have no intention to cause harm to the system. There is also a possibility that an adversary reprograms a captured node to act selfishly. The malicious node has an intention to cause maximum harm to the system, even at the cost of node's own resources. There are many types of node misbehaviors such as gray hole, black hole, routing loop, bad mouth, wormhole etc. In gray hole attack the malicious node choose the packet on the base of packet type. The malicious node may not forward the active data packet in network but may participate in routing by forwarding the routing packets. In black hole misbehavior the malicious node advertises wrongly that it has a shortest route to the destinations. After receiving the packet malicious node drops the packet. In routing loop misbehavior, the malicious node changes route information and causes routing loop in network. The routing loop may cause congestion and denial-of-service issues in network. Some malicious nodes may get together to spread false information about a normal node. Therefore, the trust rating of a well-reputed node may reduce.

In wormhole misbehavior, some nodes make a group and redirect traffic to a slow link that may cause congestion and increased latency in the network. The malicious node delays packets randomly in network and this behavior keeps the trust rating of the node above a certain threshold. Therefore, the malicious node may not be detected easily. The packet may be injected, with wrong data, such as false source and destination identifiers. In Sybil attacks, the node masquerades its identity to appear with multiple identities to represent more than one node.

Therefore, it is difficult to detect such a node acting maliciously when the node is frequently changing its identities. In transient behavior a node may alternate between the roles of being on and off to keep the repute of the node above a certain threshold. Therefore, making it hard to detect a malicious node. In ID spoof an intruder may alternatively spoof the source ID of the routed packets, leading to the disruption of routing. In such a scenario, it would also be difficult to locate the intruder node.

In node collision behavior one node plays different roles with different node groups. It can sometime misbehave with one group and behave well with another group. This creates an environment of mistrust between the two groups.

The low battery problem is the most common example of resource constraint a node may experience in a WSN. A node with low battery may participate in the route discovery process. However, the node may decline participation in packet forwarding, which renders the node indistinguishable from the packet dropping malicious nodes.

The Black hole attack is misbehavior of a node in network. A Black hole node claims itself as a suitable node for forwarding the packets to destination in the network, but actually causes dropping of packets in the network. A malicious node exploits the weaknesses of the route discovery packets of the on demand protocols, such as AODV, to drop all the packets in the network. Figure 4 shows the Black hole attack.

During the route discovery in the process of AODV protocol the intermediate nodes are accountable to find a fresh path to the destination, sending discovery packets to the neighbor nodes. When source node sends RREQ packet and Node 3, a malicious node, sends a false response to the request packet that it has the shortest route to the destination. Therefore, node1 sends its data packets via the malicious node (node 3) to the destination (node 4) assuming it is a true path. As discussed above, a malicious node most likely drops the packets, so node 3's behavior can be regarded as a Black hole problem in WSN. Due to this misbehavior, node 3 is capable of misrouting the packets easily. This type of attack severely diminishes the packet delivery ratio.

Components of trust-based system: This section discusses trust based systems components (Khalid *et al*., 2013) and elaborate each component one by one.

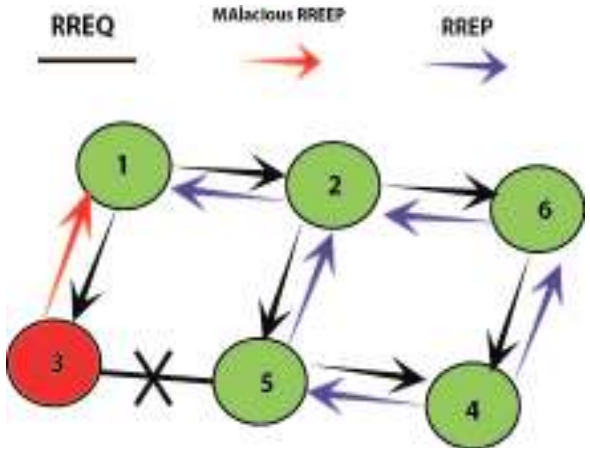

Fig. 4: Blackhole attack

Information gathering: The first component is information gathering and in this step, the nodes gather the initial trust information and then nodes observes other nodes using a watchdog mechanism. In watchdog mechanism the node must observe the neighbor in a promiscuous mode. If the neighboring node forwards the packet, then trust rating is incremented and updated in the sender node's database. On the contrary, if the neighboring node drops the packet, then trust rating is decremented in the sender node's database. In below figure the node A forwards a packet and observes node B in promiscuous mode. When node B forwards the packet, a copy of packet is also received by node A that verify the packet contents and then updates the trust rating for node B.

Information sharing: In this component, the first-hand information also known as direct trust and based on nodes experience with its neighboring node. Second hand information or indirect trust between two nodes is based on nodes own experience rather than previous trust. The second hand information is efficient, because the reputation build-up process is fast and establishes a global view of trust in the network. The nodes disseminate this second-hand information proactively or reactively. Reactively mean checking after a fixed time interval, or on the occurrence of some event or substantial change in the network. The second hand information has various benefits such as it makes the system vulnerable to false report attacks. This vulnerability can be mitigated by adopting a strategy of limited information sharing i.e.: either sharing only positive or negative information. The problem in second hand information is that while sharing only positive information makes the system vulnerable to false praise attacks. When only positive information is shared, not all the information in the system is used, since nodes cannot share their bad experiences.

In the same way, contribution the negative information prevents false praise attacks; it has its own disadvantages. Not all the information is used; nodes cannot share their good experiences. More importantly, malicious nodes can launch bad-mouth attack either individually or in collusion with other malicious nodes. CONFIDANT (Buchegger and Le Boudec, 2002) suffers from this kind of weakness. Another solution OCEAN (Bansal and Baker, 2003) for avoiding such consequences is not to share any information at all. This is one such model that builds reputation purely based on its own observations.

The convergence time of the system to build reputation is increased and it takes longer for reputation to fall, allowing malicious nodes to stay in the system longer. Systems like Distributed Reputation-based Beacon Trust System (DRBTS) and Reputation Framework for Sensor Network (RFSN) share both positive and negative information to mitigate negative effects of information sharing by incorporating first-hand and second hand information along with different weighting functions for different information (Ganeriwal *et al*., 2008).

Information mapping to the trust model: This model combines both first hand and second hand information meaningfully into a metric and maintains and updates this metric. Some models use reputation for instant Collaborative Reputation Mechanism (CORE) and Distributed Reputation-based Beacon Trust System (DRBTS). Reputation Framework for Sensor Network (RFSN) uses reputation and trust metrics. While generally, models create use of both first-hand and second-hand information in updating reputation and/or trust, some models like OCEAN use just first-hand information. The first-hand information can be directly incorporated into the reputation metric without much processing. However, this is not the case with second-hand information. The node providing the second-hand information could be malicious and ratings it provides could be spurious. Hence it is necessary to use some means of validating the credibility of the reporting node. TRMs use a selection of statistical models to evaluate the correctness of the secondhand information, depending on the application and security requirements. For instance, the model in (Ganeriwal *et al*., 2008) uses Dempster-Shafer belief theory (Shafer, 1976) and discounting belief principle (Jøsang, 2001) to incorporate second-hand information. However, Beta distribution has been the most popular among researchers in reputation and trust-based systems. It was first used by Jsang and Ismail (2002). The other statistical distributions that are used in practice are Poisson, binomial and Gaussian distributions. Another important problem in maintaining and updating reputation is how past and current information is weighted. Different models tend to weight them differently, each with a different rationale. Some Models like CORE tend to give more weight to the past observations; on the other hand, models like RFSN tend to give more weight to recent observations than the past.

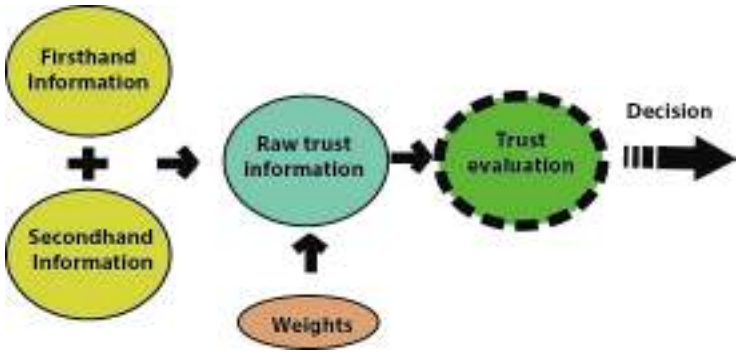

Fig. 5: Trust computation decision process (Khalid *et al*., 2013)

Decision making: The last step is decision making and based on the information provided by the information modeling component. The decision is may be one or two binary values, one is cooperate and forward the packet and a "0" is cooperating. The decision of this component varies along with the reputation and trust values in the information modeling component. The decision can vary from trust to no-trust, wherein a node that was trusted so far will no longer be trusted after its reputation and trust values fall below a predetermined threshold. Similarly, it can vary from no-trust to trust, wherein a node that to begin with was not trusted will be trusted soon after its reputation and trust values exceed a predetermined threshold (Fig. 5).

DISCUSSION

One of the major issues in current reactive routing protocols is the high resources consumption while countering packet drop. The route discovery phase of the routing process consumes bandwidth and battery power. Furthermore, such schemes severely suffer in realistic network environment from node misbehaviors like black hole, gray hole and false reporting about the nodes in the network. However, the collaboration between sensors are susceptible to malicious manipulation in WSNs. Adversaries can gain access to routing paths and redirect the traffic, or distribute false information to mislead routing direction, or flooding packets in order to block/interrupt the traffic in the network, acting as black holes to swallow (i.e., to receive but not forward) all the received messages and selectively forwarding packets through certain sensors.

Trust aware schemes: In this section, the black hole and gray hole schemes are highlighted. The gray hole attack is sometimes called selective forwarding attack. In this attack malicious nodes try to stop the packets in the network by declining to forward or dropping the messages passing through them (Zahariadis *et al*., 2010). In the forwarding attack, the malicious node can select and drop the packets, which are coming from a particular node group. The authentication and encryption can prevent some outsider attacks but these mechanisms are inefficient to detect the black hole and selective forwarding attacks.

TRUSTEE model: A TRUSTEE model is proposed to evaluate nodes behavior and for secure routing. In this scheme, the trust model evaluates nodes trustworthiness to detect compromised node. Initial trust relationship is established by node authentication and in bootstrapping phase, each sensor sends authentication messages to its neighbors which are encrypted with corresponding shared key. If the neighbor node is (denoted by node i) is legal, node i decrypts the message with corresponding shared key. Otherwise, if node i is an illegal node, node i is removed from its own neighbor set and added to its black list. Similarly, all nodes in the network will refuse to add it as a neighbor. Then the adversary is prevented from joining the topology of the network. Trust value metric is computed by packet forwarding cooperation and retransmission ratio. Packet forwarding cooperation based on MAC layer ACK a node receives from message recipient. Based on the trust metric four trust levels are maintained in range from 0 to 1. In this scheme author suggests that different data always have dissimilar significance and security levels. Based on this suggestion, four security levels in accordance with trust levels are maintained, in order to route most important data along more trusted route.

In this scheme some shortcomings are noticed. A node shares secret keys with its neighboring nodes, but when an insider attack has been made, adversary can have access to secret keys. ACK has been used to measure packet-forwarding cooperation, but a compromised node can send false ACK messages while dropping all packets. Authentication mechanism to initialize trust is suited for outsider attacks rather than insider attack, because a legal node may come under adversary attack after it has gained authentication to become part of the network.

Location-aware, trust-based detection and isolation: Another distributed trust-based framework scheme

proposed for the election of trustworthy cluster heads in a cluster-based WSN (Crosby *et al*., 2011). In this scheme the author uses location awareness and received signal strength in the validation of location information. The model uses direct information coming from trusted nodes. Trust is modeled using the traditional weighing mechanism of the parameters: packet drop rate, data packets and control packets. Each node stores a trust table for all the surrounding nodes and these values are reported to the cluster head only and upon request. This approach is not based on second-hand information, so it reduces the effect of false reporting.

Reputation based framework: Reputation based Framework for Sensor Networks (RFSN) model was proposed for a distributed trust framework for the WSNs to avoid false reporting and malicious behavior of nodes (Ganeriwal *et al*., 2008). In this framework the nodes using both first-hand and second-hand trust information. The nodes share only the positive trust information. A weight factor is applied to the second-hand information. A higher weight factor is applied to the secondhand information received from a well-reputed node. Second hand information is also included in the statistical computation of reputation. This information is gathered from nodes in the neighborhood. The inclusion of second hand information would normally imply that the protocol is susceptible to false reporting of observed behavior. However, the authors remove this attack by allowing the nodes to only propagate good reputation information about other nodes. As the authors themselves point out, this resiliency comes at the cost of system efficiency, as now the nodes cannot exchange their bad experiences about malicious/faulty nodes in the network.

Reputation-based trust model: The proposed reputation-based trust model in WSNs borrows tools from probability, statistics and mathematical analysis (Chen *et al*., 2007). The authors argued that the positive and/or negative outcomes for a certain event are not enough to make a decision in a WSN. The same approach presented in RFSN is followed; a watchdog mechanism to monitor the other nodes and to calculate the reputation and eventually to calculate trust. Bayes' theorem is used to describe the binary events, successful and unsuccessful transactions, with the introduction of uncertainty.

Weighted-trust evaluation: The Weighted-Trust Evaluation (WTE) scheme detects the compromised nodes by monitoring its reported data in WSN (Atakli *et al*., 2008). In this scheme the three-layered network architecture is assumed with three types of nodes low-power sensor with limited functionality, high-power Forwarding Nodes (FN) and Access Points (AP) or base station responsible for routing the data between wireless and wired networks. Each sensor node only communicates with its forwarding nodes FN and makes available information such as sensor reading to its FN. FNs offers multi-hop routing capability to SNs or other FNs. Each FN has two wireless interfaces, one communicates with lower layer Nodes (SNs) and the other connects to higher layer nodes (APs). To detect malicious nodes network architecture is modeled into weight-based architecture where a weight W is assigned to each sensor node. The FN collects all information provided by SNs and calculates an aggregation result using the weight assigned to each SN in Eq. (1):

$$E = \Sigma_{n=1}^{N} W_n \times U_n \quad (1)$$

where, E is the aggregation result and W_n is the weight ranging from 0 to 1. Sensor node's output may be "false" or "true" information or continuous numbers such as a temperature reading. If a sensor node's weight is lower than a specific threshold, that node is assumed as a malicious node. Some drawbacks of this scheme are: no mechanism is defined on which parameter weights are assigned to nodes, no counter measure is provided if Access Point (AP) node is captured by adversary. Also this mechanism does not exclude malicious nodes from routing path and does not perform well if number of compromised nodes are larger than the normal nodes.

BAMBI-black hole attacks mitigation with multiple base stations: One more scheme proposed and based on a technique that uses multiple base stations deployed in the network to counter the impact of black holes on data transmission (Misra *et al*., 2011). Authors assume that a set β of BSs are placed in the network. The network is connected such that every SN can reach each Bi∈ β. To ensure that every SN has a route to it, each BS Bi uses beaconing messages. BS Bi broadcasts the beacon packet with its ID as the sender ID as well as the BS ID and hop count value. Each BS monitors the received packets for $T_{monitor}$ seconds, which is a system parameter chosen based on the data frequency in the network. Even if an SN does not have any sensed data to send or forward, it periodically sends a blank data packet to the BSs to help in black hole identification. This scheme suffers from high routing overhead and network congestion.

COMPARISON OF TRUST AWARE ROUTING SCHEMES

This study also compares 15 pertinent and latest studies that propose various trust aware routing models. Different routing schemes are compared on whether

Table 1: Trust aware routing schemes comparison

Trust aware approaches	Avoid false reporting	Blackhole detection	Blackhole and grayhole detection	Other routing attacks	Direct trust only	Both direct and indirect trust	Energy consideration	Location consideration	Traffic load consideration
Ngai and Lyu (2004)	✓	×	×	×	✓	×	×	×	×
Weifang *et al*. (2006)	×	×	×	✓	×	✓	×	×	×
Crosby *et al*. (2011)	✓	×	×	×	✓	×	×	×	×
Ganeriwal *et al*. (2008)	✓	×	×	✓	×	✓	×	×	×
Stelios *et al*. (2009)	×	×	×	✓	×	✓	✓	✓	×
Gidijala *et al*. (2010)	×	×	×	✓	×	✓	✓	×	×
Zahariadis *et al*. (2010)	×	×	✓		×	✓	✓	✓	×
Reddy and Selmic (2011)	×	×	×	✓	×	✓	×	×	×
Misra *et al*. (2011)	×	✓	×	×	×	✓	×	×	×
Zhan *et al*. (2009)	×	×	×	✓	×	✓	✓	×	×
Zahariadis *et al*. (2010)	×	×	✓	×	×	✓	×	✓	×
Kim and Park (2012)	×	×	×	✓	×	✓	✓	×	✓
Leligou *et al*. (2012)	×	×	×	✓	×	✓	×	✓	×
Chakraborty and Chaki (2012)	×	×	×	✓	×	✓	✓	×	✓
Manikandan and Manimegalai (2013)	×	✓	×	×	×	✓	×	×	×

they address the 9 most common trust metrics including false reporting, black-hole detection, black-hole and gray-hole detection, routing attacks, direct trust only, direct and indirect trust, energy consideration, location consideration and traffic load considerations. The results of the comparison are summarized in Table 1. The table data clearly identifies that although some overlapping is observed among the models, however each model deals with a different set of trust metrics and trust evaluation procedures. The comparison further emphasizes the need for a more comprehensive routing scheme that addresses maximum number of trust metrics.

CONCLUSION

This study is a part of an ongoing study on security and trust aware routing schemes. In this study, the various components of the research problem were reviewed. The study highlights the challenges associated with the implementation of WSN in unattended environments. It also introduces safety issues in wireless sensor networks and the need for innovative approaches, such as trust, to solve these problems. In the concept of trust, the difference between confidence and security has been discussed. Finally, a comparison of existing trust aware routing schemes is conducted and summarized.

REFERENCES

Abd-El-Barr, M., M.M. Al-Otaibi and M.A. Youssef, 2005. Wireless sensor networks-part II: Routing protocols and security issues. Proceeding of the Canadian Conference on Electrical and Computer Engineering, pp: 69-72.

Akkaya, K. and M. Younis, 2005. A survey on routing protocols for wireless sensor networks. Ad Hoc Netw., 3: 325-349.

Akyildiz, I.F., W. Su, Y. Sankarasubramaniam and E. Cayirci, 2002. Wireless sensor networks: A survey. Comput. Netw., 38: 393-422.

Al-Karaki, J.N. and A.E. Kamal, 2004. Routing techniques in wireless sensor networks: A survey. IEEE Wirel. Commun., 11: 6-28.

Atakli, I.M., H. Hu, Y. Chen, W.S. Ku and Z. Su, 2008. Malicious node detection in wireless sensor networks using weighted trust evaluation. Proceedings of the 2008 Spring Simulation Multiconference, pp: 836-843.

Bansal, S. and M. Baker, 2003. Observation-based cooperation enforcement in ad hoc networks. Retrieved from: http://arxiv.org/pdf/cs/0307012.pdf.

Boukerche, A., B. Turgut, N. Aydin, M.Z. Ahmad, L. Bölöni and D. Turgut, 2011. Routing protocols in ad hoc networks: A survey. Comput. Netw., 55: 3032-3080.

Braginsky, D. and D. Estrin, 2002. Rumor routing algorthim for sensor networks. Proceeding of the 1st ACM International Workshop on Wireless Sensor Networks and Applications, pp: 22-31.

Buchegger, S. and J.Y. Le Boudec, 2002. Performance analysis of the CONFIDANT protocol. Proceeding of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp: 226-236.

Burgner, D.E. and L.A. Wahsheh, 2011. Security of wireless sensor networks. Proceeding of 8th International Conference on Information Technology: New Generations (ITNG, 2011), pp: 315-320.

Buttyan, L. and J.P. Hubaux, 2008. Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing. Cambridge University Press, Cambridge.

Chakraborty, M. and N. Chaki, 2012. ETSeM: A Energy-aware, Trust-based, Selective Multi-path Routing Protocol. In: Cortesi, A. *et al*. (Ed.), Computer Information Systems and Industrial Management. LNCS 7564, Springer, Berlin, Heidelberg, pp: 351-360.

Chen, H., H. Wu, X. Zhou and C. Gao, 2007. Reputation-based trust in wireless sensor networks. Proceeding of the International Conference on Multimedia and Ubiquitous Engineering (MUE'07), pp: 603-607.

Cho, J.H., A. Swami and R. Chen, 2011. A survey on trust management for mobile ad hoc networks. IEEE Commun. Surv.Tutorials, 13: 562-583.

Crosby, G.V., L. Hester and N. Pissinou, 2011. Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks. Int. J. Network Secur., 12: 107-117.

Deng, H., W. Li and D.P. Agrawal, 2002. Routing security in wireless ad hoc networks. IEEE Commun. Mag., 40: 70-75.

Gidijala, N.S., S. Datla and R.C. Joshi, 2010. A Robust Trust Mechanism Algorithm for Secure Power Aware AODV Routing in Mobile Ad Hoc Networks. In: Ranka, S. *et al*. (Eds.), Communication in Computer and Information Science. Noida, India. Springer, Berlin, Heidelberg, pp: 32-41.

He, T., J.A. Stankovic, C. Lu and T. Abdelzaher, 2003. SPEED: A stateless protocol for real-time communication in sensor networks. Proceeding of the 23rd International Conference on Distributed Computing Systems, pp: 46-55.

Heinzelman, W.R., J. Kulik and H. Balakrishnan, 1999. Adaptive protocols for information dissemination in wireless sensor networks. Proceeding of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp: 174-185.

Heinzelman, W.R., A. Chandrakasan and H. Balakrishnan, 2000. Energy-efficient communication protocol for wireless microsensor networks. Proceeding of the 33rd Annual Hawaii International Conference on System Sciences, 2: 10.

Intanagonwiwat, C., R. Govindan and D. Estrin, 2000. Directed diffusion: A scalable and robust communication paradigm for sensor networks. Proceeding of the 6th Annual International Conference on Mobile Computing and Networking, pp: 56-67.

Jøsang, A., 2001. A logic for uncertain probabilities. Int. J. Uncertain. Fuzz., 9: 279-311.

Jsang, A. and R. Ismail, 2002. The beta reputation system. Proceeding of the 15th Bled Electronic Commerce Conference, pp: 41-55.

Kaplantzis, S., N. Mani, M. Palaniswanmi and G. Egan, 2006. Security models for wireless sensor networks. Ph.D. Thesis, Centre of Telecommunications and Information Engineering, Monash University, Australia.

Khalid, O., S.U. Khan, S.A. Madani, K. Hayat, M.I. Khan, N. Min-Allah *et al*., 2013. Comparative study of trust and reputation systems for wireless sensor networks. Secur. Commun. Network., 6: 669-688.

Kim, M. and S.O. Park, 2012. Trust based sensor network clustering with load balance factors. Proceeding of the 15th International Conference on Network-based Information Systems. pp: 666-669.

Kohno, E., T. Okazaki, M. Takeuchi, T. Ohta, Y. Kakuda and M. Aida, 2012. Improvement of assurance including security for wireless sensor networks using dispersed data transmission. J. Comput. Syst. Sci., 78: 1703-1715.

Leligou, H.C., P. Trakadas, S. Maniatis, P. Karkazis and T. Zahariadis, 2012. Combining trust with location information for routing in wireless sensor networks. Wirel. Commun. Mob. Com., 12(12): 1091-1103.

Lindsey, S. and C.S. Raghavendra, 2002. PEGASIS: Power-efficient gathering in sensor information systems. Proceeding of IEEE Aerospace Conference, 3: 3-1125-3-1130.

Manikandan, S.P. and R. Manimegalai, 2013. Trust based routing to mitigate black hole attack in MANET. Life Sci. J., 10(4): 490-498.

Manjeshwar, A. and D.P. Agrawal, 2001. TEEN: A routing protocol for enhanced efficiency in wireless sensor networks. Proceeding of the IPDPS, 2001 Workshops, pp: 189.

Manjeshwar, A. and D.P. Agrawal, 2002. APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. Proceeding of the International Parallel and Distributed Processing Symposium (IPDPS, 2002), pp: 48.

Misra, S., K. Bhattarai and G. Xue, 2011. BAMBi: Blackhole attacks mitigation with multiple base stations in wireless sensor networks. Proceeding of IEEE International Conference on Communications (ICC, 2011), pp: 1-5.

Momani, M., 2010. Trust models in wireless sensor networks: A survey. In: Meghanathan, N. *et al*. (Eds.): CNSA 2010. CCIS 89, Springer-Verlag, Berlin, Heidelberg, pp: 37-46.

Ngai, E.C.H. and M.R. Lyu, 2004. Trust- and Clustering-based Authentication Services in Mobile Ad Hoc Networks. Proceeding of the 24th International Conference on Distributed Computing Systems Workshops, pp. 582-587.

Niezen, G., G.P. Hancke, I.J. Rudas and L. Horvath, 2007. Comparing wireless sensor network routing protocols. Proceeding of the AFRICON 2007, pp: 1-7.

Nikjoo, S., A.S. Tehrani and P. Kumarawadu, 2007. Secure routing in sensor networks. Proceeding of Canadian Conference on Electrical and Computer Engineering (CCECE, 2007), pp: 978-981.

Nivetha, G. and K. Venkatalakshmi, 2012. Comparative analysis on routing techniques in wireless sensor networks. Int. J. Adv. Res. Electron. Commun. Eng., 1: 61-67.

Pal, S., D. Bhattacharyya, G.S. Tomar and T.H. Kim, 2010. Wireless sensor networks and its routing protocols: A comparative study. Proceeding of International Conference on Computational Intelligence and Communication Networks (CICN, 2010), pp: 314-319.

Pathan, A., H.W. Lee and C.S. Hong, 2006. Security in wireless sensor networks: Issues and challenges. Proceeding of the 8th International Conference Advanced Communication Technology (ICACT, 2006), 6: 1048.

Perrig, A., J. Stankovic and D. Wagner, 2004. Security in wireless sensor networks. Commun. ACM, 47: 53-57.

Reddy, Y.B. and R.R. Selmic, 2011. A trust-based approach for secure packet transfer in wireless sensor networks. Int. J. Adv. Secur., 4(3): 198-207.

Rodoplu, V. and T.H. Meng, 1999. Minimum energy mobile wireless networks. IEEE J. Sel. Area. Comm., 17: 1333-1344.

Sen, J., 2009. A survey on wireless sensor network security. Int. J. Commun. Netw. Inform. Secur., 1(2).

Shafer, G., 1976. A Mathematical Theory of Evidence. Princeton University Press, Princeton, Vol. 1.

Sharma, G., A. Verma and V. Bhalla, 2009. Routing in wireless sensor networks. M.A. Thesis, Computer Science and Engineering Department, Thapar University, Patiala, India.

Sohrabi, K., J. Gao, V. Ailawadhi and G. J. Pottie, 2000. Protocols for self-organization of a wireless sensor network. IEEE Pers. Commun., 7: 16-27.

Srinivasan, A., J. Teitelbaum, J. Wu, M. Cardei and H. Liang, 2009. Reputation-and-trust-based systems for ad hoc networks. Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks, pp: 375.

Stavrou, E. and A. Pitsillides, 2010. A survey on secure multipath routing protocols in WSNs. Comput. Netw., 54: 2215-2238.

Stelios, Y., N. Papayanoulas, P. Trakadas, S. Maniatis and H.C. Leligou *et al*., 2009. A distributed energy-aware trust management system for secure routing in wireless sensor networks. In: Granelli *et al*. (Eds.), MOBILIGHT 2009. Lnicst 13, Springer, Berlin, Heidelberg, pp: 85-92.

Wang, Y., G. Attebury and B. Ramamurthy, 2006. A survey of security issues in wireless sensor networks. IEEE Commun. Surv. Tutorials, 8(2): 2-23.

Weifang, C., L. Xiangke, S. Changxiang, L. Shanshan and P. Shaoliang, 2006. A trust-based routing framework in energy-constrained wireless sensor networks. In: Cheng, X., W. Li and T. Znati (Eds.), Wireless Algorithms, Systems, and Applications. LNCS 4138, Springer-Verlag, Berlin, Heidelberg, pp: 478-489.

Wood, A. and J.A. Stankovic, 2002. Denial of service in sensor networks. Computer, 35: 54-62.

Xu, Y., J. Heidemann and D. Estrin, 2001. Geography-informed energy conservation for ad hoc routing. Proceeding of the 7th Annual International Conference on Mobile Computing and Networking, pp: 70-84.

Yahya, B. and J. Ben-Othman, 2009a. An energy efficient and QoS aware multipath routing protocol for wireless sensor networks. Proceeding of IEEE 34th Conference on Local Computer Networks (LCN, 2009), pp: 93-100.

Yahya, B. and J. Ben-Othman, 2009b. REER: Robust and energy efficient multipath routing protocol for wireless sensor networks. Proceeding of IEEE Global Telecommunications Conference (GLOBECOM, 2009), pp: 1-7.

Yao, Y. and J. Gehrke, 2002. The cougar approach to in-network query processing in sensor networks. Sigmod Rec., 31: 9-18.

Yu, Y., R. Govindan and D. Estrin, 2001. Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks. Technical Report ucla/csd-tr-01-0023, UCLA Computer Science Department 2001.

Zahariadis, T., H.C. Leligou, P. Trakadas and S. Voliotis, 2010. Trust management in wireless sensor networks. Eur. T. Telecommun., 21: 386-395.

Zhan, G., W. Shi and J. Deng, 2009. SensorTrust: a resilient trust model for WSNs. Proceeding of the 7th ACM Conference on Embedded Networked Sensor Systems, pp: 411-412.