Security Analysis of Routing Protocols in Wireless Sensor Networks

Mohammad Sadeghi[1], Farshad Khosravi[2], Kayvan Atefi[3], Mehdi Barati[4]

[1]Faculty of Computer and Mathematical Sciences, UiTM,
Shah Alam, Malaysia

[2]Faculty of Electrical Engineering, Islamic Azad University
Eslam Abad Gharb,Iran

[3]Faculty of Computer and Mathematical Sciences, UiTM,
Shah Alam, Malaysia

[4]Faculty of Computer Science, UPM, Malaysia

Abstract

In this paper, I describe briefly some of the different types of attacks on wireless sensor networks such as Sybil, HELLO, Wormhole and Sinkhole attacks. Then I describe security analysis of some major routing protocols in wireless sensor network such as Directed Diffusion, TinyOS beaconing, geographic and Rumor routings in term of attacks and security goals. As a result I explain some secure routing protocols for wireless sensor network and is discussed briefly some methods and policy of these protocols to meet their security requirements. At last some simulation results of these protocols that have been done by their designer are mentioned.

Keywords: *Security Analysis, Routing Protocols, Wireless Sensor Networks (WSN), attacks in network*

I. INTRODUCTION

Wireless sensor networks (WSNs) have gained worldwide interest in these years. Advances in Microelectronic Systems and low power radio technologies have created low-cost, low-power, multi-functional sensors devices, which can sense, measure, and collect information from the environment and transmit the sensed data to the user by a radio transceiver. Sensor nodes can use battery as a main power source and harvest power from the environment like solar panels as a secondary power supply.

An unstructured WSN is a network that contains a dense collection of sensor nodes and can be automatically organized to form an ad hoc multihop network to communicate with each other. On the other hand, a structured WSN deploys all or some of the sensor nodes in a pre-planned manner. So, it has a lower network maintenance and management cost.

WSNs can be used for many applications such as military target tracking and surveillance, natural

disaster relief, biomedical health monitoring, environment exploration and agricultural industry [5]. The architecture of commonly used WSN is as depicted in figure 1.

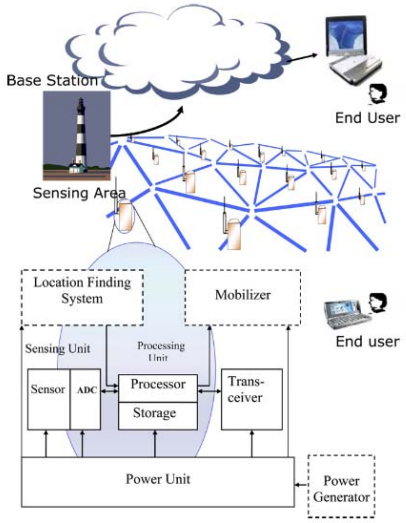

Fig.1 The architecture of commonly used in WSN

Wireless sensor networks like any wireless technology are susceptible to several security attacks due to the broadcast nature of transmission medium [1]. There are constraints in incorporating security into a WSN such as limitations in storage, communication, computation, and processing capabilities. To Design a security protocol we need to understand these limitations and achieve acceptable performance with security measures to meet the needs of an application.

In this paper, I describe briefly some of the different types of attacks on wireless sensor networks and also security analysis of some major routing protocols in wireless sensor network in term of design and security goals.

II. THREAT MODEL

Attacks on wireless sensor network can be classified to mote-class attacks and laptop-class attacks. In the mote-class attacks, the attacker has access to a few sensor nodes with similar capabilities. On the other hands, a laptop-class attacker may have access to more powerful devices, like laptops or their equivalent. They may have greater battery power, a more capable CPU, a high-power radio transmitter, or a sensitive antenna and can do more than an attacker with only ordinary sensor nodes [3].

Another classification in attacks on wireless sensor network is based on the outsider or insider attacks. In insider attack a compromised node was captured by an adversary and may possess all the secret keys and be capable of participating in the communications and disrupting the network.

In contrast, outsider attacks, where the attacker has no special access to the sensor network. The outsider attacks are achieved by unauthorized nodes that can easily eavesdrop on the packets exchanged between sensor nodes due to the shared wireless medium [2].

Based on the network layers, [6] cites another classification of attacks on wireless sensor network.

Attacks at physical layer: Jamming is one of the most important attacks at physical layer. Aiming at interfering with normal operations, an attacker may continuously transmit radio signals on a wireless channel. An attacker can send high-energy signals in order to effectively block wireless medium and to prevent sensor nodes from communicating. This can lead to Denial-of-Service (DoS) attacks at the physical layers.

Attacks at link layer: The functionality of link layer protocols is to coordinate neighboring nodes to access shared wireless channels and to provide link abstraction to upper layers. Attackers can deliberately violate predefined protocol behaviors at link layer. For example, attackers may induce collisions by disrupting a packet, cause exhaustion of nodes' battery by repeated retransmissions, or cause unfairness by abusing a cooperative MAC layer priority scheme. All these can lead to DoS attacks at the link layers.

Attacks at network layer: In WSNs, attacks at routing layer may take many forms. This kind of attacks will be discussed in following.

Attacks targeting at WSN services and applications: basically, to prevent this kind of attack localization and aggregation are used.

III. ATTACKS ON ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS

Some of network layer attacks on wireless sensor networks are listed as follow:

*A) **Eavesdropping**:*

Since transport medium in wireless sensor network use broadcasting feature, so any adversary with a strong receiver could eavesdrop and intercept transmitted data. Information like location of node, Message IDs, Node IDs, timestamps, application specific information can be retrieve by an intruder. To prevent these problems we should use strong encryption techniques [1].

B) Denial of service:

In a Denial-of-Service (DoS) attack, an adversary attempts to disrupt, corrupt or destroy a network. It reduces or eliminates a network's capacity to perform its expected function [2].

C) Message tampering:

Malicious nodes can tamper with the received messages thereby altering the information to be forwarded to the destination. At the destination side, the Cyclic Redundancy Code (CRC) would be computed. The redundancy check fails and it would result in dropping the packet. If the CRC check was successful then the destination node would accept wrong information [2].

By spoofing or altering or replaying routed information, false messages can be generated, routing loops can be created, latency of the network can be increased, etc. The motivation for mounting a replay attack is to encroach on the authenticity of the communication in WSNs [7].

D) Selective forwarding:

In a selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. A simple form of this attack is when a malicious node behaves like a black hole and refuses to forward every packet she sees. By this, neighboring nodes will conclude that she has failed and decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing packets originating from a select few nodes can reliably forward the remaining traffic and limit suspicion of her wrongdoing.

Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow. However, it is conceivable an adversary overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest [3].

E) Sinkhole attacks:

In a sinkhole attack, the adversary manipulates the neighbouring nodes to attract nearly all the traffic from a particular area through a compromised node and create a sink as shown in figure 2. This malicious sink can now not only tamper with the transmitted data but can also drop some vital data and lead to other attacks like eavesdropping and selective forwarding. Sinkhole attacks usually make a compromised node that is more attractive to neighbouring sensor nodes than the routing algorithm. This could be approached by spoofing or replaying an advertisement for an extremely high quality route to a sink. Therefore, all the surrounding node of the adversary will start forwarding packets destined for a sink through the adversary, and also propagate the attractiveness of the route to their neighbours [2].

[3] Noted that the reason sensor networks are particularly susceptible to sinkhole attacks is due to their specialized communication pattern. Since all packets share the same ultimate destination, a compromised node needs only to provide a single high quality route to the base station in order to influence a potentially large number of nodes.

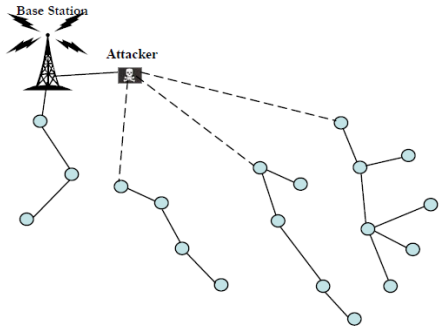

Fig.2: Sinkhole attacks

F) Wormhole attacks:

In this kind of attack, an adversary receives messages by making a tunnel and a low-latency link in one part of the network and replays them in a different part as shown in figure 3. An adversary could convince nodes who would normally be multiple hops from a sink that they are only one or two hops away via the wormhole. This would not only make some confusion in the routing mechanisms but would also create a sinkhole since the adversary on the other side of the wormhole can pretend to have a high quality route to the sink, potentially drawing all traffic in the surrounding area. An adversary that is situated near the sink may be able to completely disrupt routing by creating a well-placed wormhole [2].

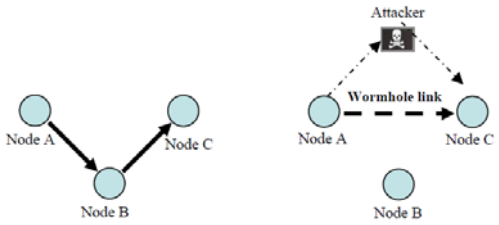

Fig.3: Normal Network (left), Wormhole Attack (right)

G) Sybil attacks:

In a Sybil attack, a single malicious node illegitimately presents multiple identities to other nodes in the network. The Sybil attack can significantly decrease the effectiveness of fault-tolerant schemes such as distributed storage, disparity and multipath routing, and topology maintenance. The Sybil attacks can take advantage of different layers to make service disruption. This attack at the routing layer will help the malicious node to draw in large amounts of network traffic to go through the same entity. This creates a sinkhole and as a result the attacker can do selective forwarding on received data [2].

In addition to defeating distributed data storage systems, the Sybil attack is also effective against routing algorithms, data aggregation, voting, fair resource allocation and foiling misbehavior detection. Regardless of the target all of the techniques involve utilizing multiple identities. For example, in a sensor network voting scheme, the Sybil attack might utilize multiple identities to generate additional “votes” [4].

H) HELLO Attack:

Nodes in WSNs learn about their neighboring nodes through HELLO packets. Every node advertises its presence to neighboring nodes by broadcasting HELLO packets. In HELLO attack, a malicious node follows the same technique. It uses transmission power high enough to reach the nodes that are very far away from its physical location which convinces the receivers of its advertised packets that it is a legitimate neighboring node as shown in Figure 4. Generally routing protocols of WSN depend on localized exchange of routing information to maintain routing topology and flow control [3].

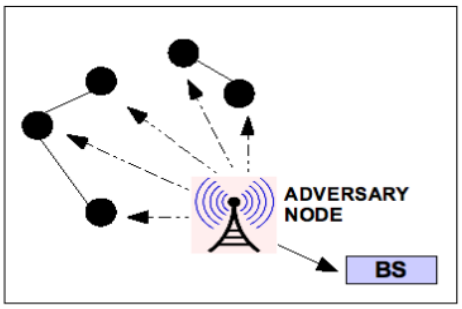

Fig. 4: HELLO attack

I) Acknowledgement spoofing:

Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements. An adversary can spoof link layer acknowledgment for ''overheard'' packets addressed to neighboring nodes to convince the sender that a weak link is strong or that a dead or disabled node is alive. By this attack a routing protocol may select the next hop in a path using link reliability [3].

IV. ANALYSIS OF ROUTING PROTOCOLS IN WIRELESS SENSOR NETWORKS IN TERM OF ATTACKS AND COUNTERMEASURES

All of the proposed sensor network routing protocols are highly susceptible to attack [3]. Some important routing protocols and relevant attacks will be discussed in following.

A. Directed diffusion

As [7] cites, Directed Diffusion is a data centric protocol for drawing information out of a sensor network. The base station asks for data by broadcasting interests. An interest is a task request that needs to be done by the network. Among the route, nodes keep propagating the interests until the nodes that can satisfy the interests are reached. Each node that receives the interests sets up a gradient toward the origin node. A gradient contains an attribute value and direction. As shown in Figure 5 when node B receives an interest from node A, it includes A(Δ) in its gradient. When node C receives an interest from node A through node B, it includes B(2Δ) in its gradient. On the other hand, when node C receives an interest from node A, it includes A(Δ) in its gradient. When the data matches the interest (event), path of information, flows to the base station at low data rate. Then the base station recursively reinforces one or more neighbors to reply at a higher data rate. Alternatively, paths may be negatively reinforced as well.

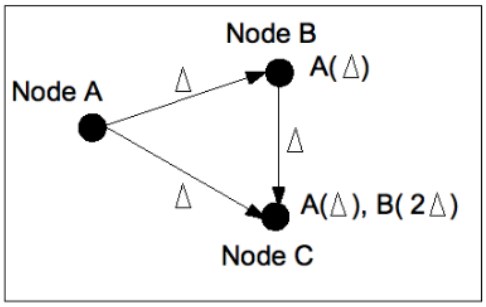

Fig. 5: Gradient set up in Directed Diffusion Routing Protocol

There is a multipath variant of directed diffusion as well. After the primary dataflow is established using positive reinforcements, alternate routes are recursively established with maximal disjointedness by attempting to reinforce neighbors not on the primary path [8].

It becomes an easy task for the attacker to eavesdrop the interest in this protocol. After an adversary receives an interest flooded from a legitimate base station, it can simply replay that interest with herself listed as a base station. When the response for that interest is sent, apart from the base station, the adversary would also be receiving them [7], [3].

When sources begin to generate data events, an adversary node might attack a data flow and cause to flow suppression. It is an instance of denial-of-service attack. The easiest way to suppress a flow is to spoof negative and positive reinforcements. It can also influence the path taken by a data flow. For instance, after receiving and rebroadcasting an interest, an adversary interested in directing the resulting flow of events through herself would strongly reinforce the nodes to which the interest was sent while spoofing high rate, low latency events to the nodes from which the interest was received. By using the above attack to insert herself onto the path taken by a flow of events, an adversary can gain full control of the flow. She can modify and selectively forward packets of her choosing [3].

On the other hand a laptop-class adversary can exert greater influence on the topology by creating a wormhole between one node that located next a base station and other node located close to where events are likely to be generated. Interests advertised by the base station are sent through the wormhole [7].

[3] Shows that the combination of the positive and negative reinforcements pushes data flows away from the base station and towards the resulting sinkhole.

A single adversary can use the Sybil attack against her neighbors even in the multipath version. A neighbor will be convinced it is maximizing diversity by reinforcing its next most preferred neighbor not on the primary flow when in fact this neighbor is an alternate identity of adversary [3].

B. TinyOS beaconing

This protocol builds a spanning tree with a base station as the parent for all the nodes in the network. Periodically the base station broadcasts a route update to neighbors which in turn they broadcast it to their neighboring nodes. All nodes receiving the update mark the base station as its parent and rebroadcast the update. The algorithm continues recursively with each node marking its parent as the first node from which it hears a routing update. All packets received or generated by a node are forwarded to its parent until they reach the base station [3].

As [7] and [3] show, the simplicity of this protocol makes it susceptible to all the attacks discussed in the previous section. Since routing updates are not authenticated, it is possible for any node to claim to be a base station and can become the parent of all nodes in the network. Authenticated routing updates will prevent an adversary from claiming to be a base station, but a powerful laptop class adversary can still carry out HELLO flood attacks by transmitting a high power message to all the nodes and by making every node to mark the adversary as the parent node.

An adversary interested in eavesdropping on, modifying, or suppressing packets in a particular area can do so by mounting a combined wormhole or sinkhole attack. The adversary first creates a wormhole between two colluding laptop-class nodes, one near the base station and one near the targeted area. The first node forwards authenticated routing updates to the second through the wormhole and rebroadcasts the routing update in the targeted area. Since the routing update through the wormhole will likely reach the targeted area considerably faster, the second node will create a large routing subtree in the targeted area with itself as the root [3]. As you can see in Figure 6 it might cause to selective forwarding attack.

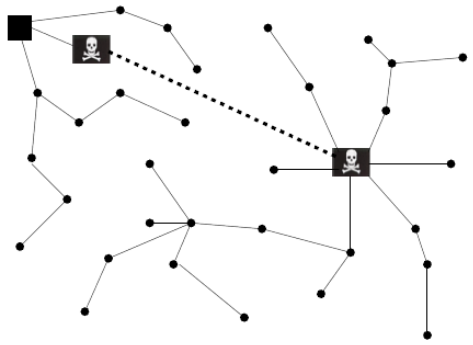

Fig. 6: A laptop-class adversary using a wormhole to create a sinkhole

C. Geographic routing

Geographic and Energy Aware Routing (GEAR) [9] and Greedy Perimeter Stateless Routing (GPSR) [10] use nodes' positions and informed neighbor selection heuristics and also explicit geographic packet destinations to efficiently disseminate queries and route replies in the sensor network. GPSR uses greedy forwarding at each hop, routing each packet to the neighbor closest to the destination. During the routing, when some holes appear and greedy forwarding becomes impossible, GPSR recovers by routing around the perimeter of the void. One of the GPSR problems is that packets along a single flow will always use the same nodes for the routing of each packet, leading to uneven energy consumption.

GEAR attempts to solve this problem by weighting the choice of the next hop by both remaining energy and distance from the target. Every node has two different costs for accessing a destination. First, an estimated cost that is a mixture of residual energy in the power supply (battery) and its distance to the destination; and the second one, a learning cost that accounts for routing when the holes happens in the network. A hole is formed when there is no other node closer to the target other than itself. When a node receives a packet, it checks whether any of its neighbors is located closer to the target region. If there are more than one, the one that is closest to them target is chosen. If there is only one, it hoses that node. If there isn't any, then there is a hole and it picks one of its neighbors based on the learning cost function. So, both GEAR and GPSR protocols require location (and energy for GEAR) information to be exchanged between neighbors.

Location and cost information can be misrepresented. Attacks can be launched by an adversary node by just advertising to have maximum energy. For instance, in GEAR, an appropriate attack would be to always advertise maximum energy as well. An adversary can also

significantly increase her chances of success by mounting a Sybil attack. It can carry out Sybil attack by covering up the target node with multiple bogus nodes [3].

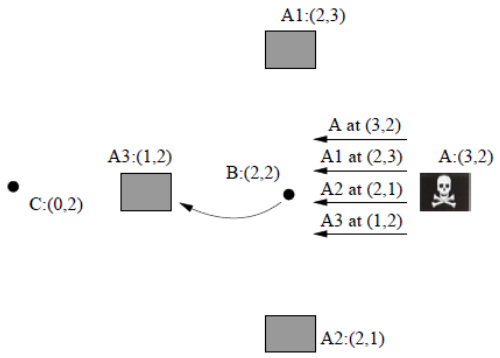

Fig. 7: The Sybil attack against geographic routing.

As shown in Figure 7, Adversary A at actual location (3,2) forges location advertisements for non-existent nodes A1, A2, and A3 as well as advertising her own location. After hearing these advertisements, if B wants to send a message to destination (0,2), it will attempt to do so through A3. This transmission can be overheard and handled by the adversary A. Once on that path, the adversary can mount a selective forwarding attack.
In GPSR an adversary can forge location advertisements to create routing loops in data flows without having to actively participate in packet forwarding [3].

D. Rumor routing

Rumor routing [11] is a probabilistic protocol for matching queries with data events. Rumor routing offers a energy efficient alternative when the high cost of flooding cannot be justified. Rather than flooding the entire network to match information with interest (event), this protocol uses long lived packets called agents. When a source node observes an event it generates an agent. Agents pass through the whole network and propagate information about the local events to distant nodes. Agents carry information such as a list of events, next hop path to those events, hop count of those paths, a list of previously visited nodes and a Time To Live (TTL) field. On arriving at a new node the agent informs that node about the events it knows and adds to its event list. It decrements it's TTL field. If TTL is more than zero the node probabilistically selects the agent's next hop from its neighbors in the routing table minus the previously visited nodes by the agent.

In the same way the base station creates an agent to propagate the query into the network. A route from a base station to a source is established when a query agent arrives at a node previously traversed by an event agent that satisfies the query in the network [7].
As explain above, this protocol is dependent on nodes forwarding the agents properly. An adversary can mount a denial-of-service attack by removing event information carried by the agent or by refusing to forward agents entirely. Query or event information in agents can also be modified.
Laptop class attackers can carry out Sybil attacks and selective forwarding attacks [7].
Mote-class adversaries can mount a selective forwarding attack by extending tendrils in all directions to create a sinkhole. It creates tendrils by forwarding multiple copies of a received agent.
The easiest way to mount a selective forwarding attack is to be on the path of the data flow. Thus, the intersection of the query and events agents must occur downstream from the adversary. So, she will be "cut out" of the path of data flow [3].

V. SECURE SENSOR NETWORK ROUTING PROTOCOLS

Enforcing security in existing routing protocols through public key cryptographic mechanisms would either make them more complex or would consume the resources of tiny sensor devices.
According to these constraints, many secure routing protocols implement symmetric key cryptographic mechanisms to provide security. But this security is not complete because they consider only few of the design principles. For instance, SPINS and TinySec focus only on Prevention principle. They provide inadequate security in the presence of compromised nodes. As a preventive measure Secure Implicit Geographic Forwarding (SIGF) protocol chooses next hop dynamically and non-deterministically rather than maintaining routing tables [7].
On the other hands, Intrusion-Tolerant Routing protocol for Wireless Sensor Networks (INSENS) protocol uses multipath technique in order to make the network resilent to attacks.
Based on the [3], none of the proposed symmetric key based routing protocols incorporate all the three main design principles. These principles are Prevention, Detection or Recovery and Resilience. So to design and build a new protocol needs to consider all the discussed requirements.
Parno et al. has designed 'Secure Sensor Network Routing Protocol with a new asymmetric key based routing protocol and also security and efficiency as the central design parameters .The overhead and complexity of cryptographic mechanisms has been observed to be within acceptable limits [7].

DAWWSEN (Defence mechanism Against Wormhole attacks in Wireless Sensor Networks) was introduced by Kaissi, R. and his group. They presented a defence mechanism against wormhole attacks in wireless sensor networks. Specifically, a simple routing tree protocol is proposed and shown to be effective in defending against wormhole attacks [2].

A proactive routing protocol based on the construction of a hierarchical tree where the base station is the root node, and the sensor nodes are the internal nodes of the tree. Each node receiving a request packet inserts a new entry in its "request list". Then the node sends a reply packet and updates its "replay table". Then the last 2 fields are set to zero. The node keeps listening to the transmitted reply packets, and increments the Num_Rep field for each received packet. Now the source node sends for each entry in its reply list an equivalent accept packet. The node receiving an accept packet should check the source ID that should be the same as the NodeID in its replay table. If this is not the case, this will mean that this packet was stored by an attacker should be dropped. If not, the node updates its replay table by setting the "Recv_accept" field to one and checks if the "Num_reply" field in the accept packet is one value greater than "Num_Rep" in the replay table of this node " Num_reply = Num_Rep + 1 ". If equation is verified, the node receiving the accept packet marks the originator of this packet as its parent, updates its routing table with the ID and the hop count of this parent and rebroadcasts a request packet with a hop count field incremented. And If the equation is not verified, a wormhole attack is detected by this node drop the received accept packet and add the ID of the originator of the accept packet to its NAP (Not Accepted Packets) table [2].

All of these routing protocols that were explained used a special simulation environment to run the simulations and evaluate the performance of the routing protocol. One of the most important of these simulators is network simulator 2 (ns2). It is a standard experiment environment in research community and creates some output files and collects statistical data synchronized from the sensor network [12].

VI. CONCLUSIONS

Wireless Sensor Networks would be widely deployed in future mission-critical applications. As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required of these wireless sensor network applications. One of these considerations is security in routing protocol of wireless sensor network.

As I explained, some designs of sensor network routing protocols satisfy security goals of wireless sensor network. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defense against mote-class outsiders, but cryptography is not enough to defend against laptop-class adversaries and insiders.

In contrast, according to my explanation, some currently proposed routing protocols for these networks are insecure. Table 1 shows briefly some attacks on these protocols.

Routing protocol	Selective Forwarding	Spoofed Attack	Sybil Attack	Sink Hole Attack	HELLO Attack
Directed diffusion	✓	✓	✓	✓	✓
TinyOS beaconing	✓	✓	✓	✓	✓
Geographic routing	✓	✓	✓	•	•
Rumor routing	✓	✓	✓	✓	•

Table 1: Summary of Attacks on routing protocols in Wireless Sensor Network

So, security problems at routing layer have to be resolved before their deployment in real world situations. A secure routing protocol should possess preventive measures against known attacks. Secure Sensor Network Routing protocol provides good security against all known attacks.

On detection of any suspicious activity of a malicious node recovery mechanisms should be triggered. Stability of the network should not be drastically disturbed even in the presence of the malicious node. Some secure routing protocols were explained and on implementing these protocols in particular operating system environment, it has been observed that the performance overhead is within acceptable limits compared to the level of security achieved.

REFERENCES

[1] J. Yick, B. Mukherjee, and D. Ghosal., *Wireless Sensor Network Survey*, 2008.

[2] R. El-Kaissi, A. Kayssi, A. Chehab, and Z. Dawy., *DAWWSEN: A Defence mechanism Against Wormhole attacks in Wireless Sensor Networks.*

[3] C. Karlof and D. Wagner, *Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,* University of California at Berkeley.

[4] J. Paul Walters, Z. Liang, W. Shi, and V. Chaudhary, *Wireless Sensor Network Security: A Survey,* Department of Computer Science Wayne State University.

[5] S. Tripathy and S. Nandi, *Defense against outside attacks in wireless sensor networks,* Department of Information Technology, North Eastern Hill University, October 2007.

[6] B. Sun, Y. Xiao, Ch. Chih Li, T. Andrew Yang, *Security co-existence of wireless sensor networks and RFID for pervasive computing*, Department of Computer Science, Lamar University, USA.
[7] S. Shanmugham, *Secure Routing in Wireless Sensor Networks* Scholarly Paper Advisor: Dr. Jens-Peter Kaps.
[8] C. Intanagonwiwat, R. Govindan, and D. Estrin, *Directed diffusion: A scalable and robust communication paradigm for sensor networks,* in Proceedings of the Sixth Annual International Conference on Mobile Computing and Networks, August 2000.
[9] Y. Yu, R. Govindan, and D. Estrin, *Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks,* University of California at Los Angeles Computer Science Department, May 2001.
[10] B. Karp and H. T. Kung, *GPSR: greedy perimeter stateless routing for wireless networks*, in Mobile Computing and Networking, 2000.
[11] D. Braginsky and D. Estrin, *Rumour routing algorithm for sensor networks,* in First ACM International Workshop on Wireless Sensor Networks and Applications, 2002.
[12] J. Wang, *ns-2 Tutorial,* Multimedia Networking Group, The Department of Computer Science, 2004