Threats and Attacks Analysis of Routing Protocols for Wireless Sensor Networks

Riyazahmed A Jamadar[1], Mousami. S Vanjale[2]

[1]ME Research Scholar, Department of Electronics, AISSMS IOIT, Pune

[2]Assistant Professor, Department of Electronics, AISSMS IOIT, Pune, Ph.d Research Scholar BVD University Pune

Abstract: ***In this paper, we emphasize and discuss some attacks on wireless sensor network which are of crucial significance to the performance and existence of it. The wireless sensor networks are resource constrained, more particularly power and memory. Attacks such as Sybil, HELLO, Wormhole and Sinkhole basically target routing of packets and degrade the throughput and performance of network by draining out power and memory. This paper underlines and describes the need of robust routing protocols to secure the wireless sensor network against such attacks. A comprehensive study of existing protocols such as Directed Diffusion, TinyOS beaconing, Geographic and Rumor routings is been presented here along with future research scope.***

Keywords: Wireless Sensor network, Threat Analysis,Routing Protocol,Performance.

1. Introduction

The advent of cutting edge technologies like VLSI and Wireless Communications have made Wireless sensor networks (WSNs) to develop feasible and affordable systems for military, health care and agriculture. These have gained worldwide interest in these years. Basically WSNs employ battery as a primary power source and harvest power from the environment like solar panels as a secondary power supply. The goal of adversary may to steal the information or to create disorder in the functioning of the WSN there by targeting draining out of these resources.

Security and Privacy are important challenges in all types of wired and wireless communications. These

are of prime importance in wireless sensor networks, where the unique characteristics of these networks make them attractive targets for intrusions and other attacks. These attacks have serious consequences if any breach of security, compromise of information, or disruption of correct application behavior on, applications such as battlefield surveillance, target tracking, monitoring civil infrastructure, and assessment of disaster zones to guide emergency response activities etc.

As WSNs are frequently used in remote areas and laid to operate unattended networks , they provide an easy target for physical attacks, tampering and unauthorized access. WSNs are typically very resource-constrained and operate in harsh environments, which further facilitate compromise and make it often difficult to distinguish security breaches from node failures, varying link qualities, and other commonly found challenges WSNs.

So, these resource constraints require secured routing mechanisms that are customized for WSN applications. So in the first part we discuss different types attacks in WSNs and their impact on performance, secondly an Analysis of existing routing protocols like Directed Diffusion, TinyOS beaconing, Geographic Routing and Rumor Routing is been made in the presence of adversities[13]. This paper uses terms attacker, intruder, and adversary interchangeably to describe an person that performs an attack on a network or system.

2. Types of Attacks in WSN

Basically we find two types of attacks in WSNs, namely, mote-class attacks and laptop-class attacks. In the mote-class attacks, the attacker has access to a some sensor nodes with similar capabilities.In the latter type an 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].

The other way attacks on wireless sensor network could be classified 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 outsider attacks, an 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.

Link layer attacks: 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 purposely violate predefined protocol behaviors at link layer. For instance, attackers may induce collisions by disrupting a packet, cause exhaustion of node's 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.

Network layer attacks: In WSNs, attacks at routing layer may take many forms. This kind of attacks will be discussed in following. Attackstargeting at WSN services and applications: basically, to prevent this kind of attack localization and aggregation are used. Some of network layer attacks on wireless sensor networks are listed as follow:

a) Eavesdropping

As transport medium in wireless sensor network uses broadcasting feature, the adversary could eavesdrop and intercept transmitted data easily. 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 [2].

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 this type of 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 adjacent 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 adjacent 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]. 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.

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].

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].

Bsides 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 [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].

3. 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].

4. Analysis of Routing Protocols in WSNS

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.

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

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.

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.

c) Geographic Routing

Geographic Routing is based on greedy forwarding principle. Geographic and Energy Aware Routing (GEAR) [9] and Greedy Perimeter Stateless Routing

(GPSR) [10] use node's 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.

d) Rumor Routing

Rumor routing is one of the widely employed routing protocol in WSNs. 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 , 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.

5. 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. 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.

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

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

Some secured routing protocols were discussed and on implementing these protocols in particular WSN based operating systems environment, it has been observed deviated performance of attacks.

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 ervasive 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, ay 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

[13] Waltenegus Dargie Technical University of Dresden, Germany Christian Poellabauer University of Notre Dame, USA. Fundamentals of Wireless SENSOR Networks. Theory and Practice