Security Threats in Wireless Sensor Networks

Hiren Kumar Deva Sarma
Sikkim Manipal Institute of Technology
&
Avijit Kar
Jadavpur University

ABSTRACT

Wireless Sensor Network (WSN) is an emerging field. These are normally designed to perform a set of high level information processing tasks; for example, detection, tracking, or classification. Different application areas of WSNs are Environmental Monitoring, Industrial Sensing and Diagnostics, Infrastructure Protection, Battlefield Awareness, Context Aware Computing, etc. From application areas of WSN, it has been observed that ensuring security and privacy is one of the highest priorities for Wireless Sensor Network Systems. Information in the network must be protected from attackers. Attackers may devise different types of security threats to make the WSN system unstable. Herein, we have identified different security threats possible for a Sensor Net Setting. Effort has been made to model the threats mathematically. Future scope of the work has also been outlined.

INTRODUCTION

Wireless Sensor Networks have emerged as a dominant technology in the current decade. Diversified application areas of Wireless Sensor Networks indicate the bright future of this new paradigm. WSNs are becoming popular day by day. Already many companies have started developing commercial applications. At the same time they have posed numerous unique challenges to researchers. Wireless sensor networks are generally composed of hundreds or even thousands of tiny sensor nodes, which are constrained in many aspects like memory capacity, processing power, and most importantly, energy or battery power. Most of the time sensor nodes do not have access to renewable energy resources. The overall cost of a WSN is also required to be relatively lower.

Moreover when we look at the applications of WSNs, there are many applications areas, e.g., battlefield awareness, traffic monitoring system, etc., in which security of information remains as an important issue. Providing security to a WSN is a nontrivial problem. Security mechanisms which are applicable of being wired or other ad-hoc networks are not suitable for WSN. There are many reasons behind it and we discuss those in subsequent sections.

Though there are varieties of challenges in sensor networks, herein we focus on different security issues and possible remedies.

To make WSN feasible for all kinds of applications at lower cost we need simple protocols for communication, security, topology management, medium access control which are supposed to be energy efficient. Though security is a very important issue in WSN, very little work is available for securing a WSN. To understand the limitations of current security mechanisms, it is necessary to realize the features of a wireless sensor network. Different features of WSN such as low memory, low energy, low bandwidth for communication, and large scale nodes make most of the current security solutions available for other ad hoc and wired networks impractical for WSNs.

We have identified different challenges in providing security to a WSN deployment.

The First Challenge:

There is a conflicting interest between minimization of resource consumption and maximization of security level. A better solution actually gives a. good compromise between these two. During the design of any security solution we need to take care of following resource constraints [1]:

- limited energy,
- limited memory,

Author's Current Address:
H. Kumar, D. Sarma, Department of IT, Sikkim Manipal Institute of Technology, Majitar. PO-Rangpo, East Sikkim, India Pin 737132; and A. Kar, Department of CSE, Jadavpur University, Kolkata, India Pin 700 032.

Based on a presentation at Carnahan 2006.

- limited computing power;
- limited communication bandwidth; and
- limited communication range.

The Second Challenge:
The type of security mechanism that can be hosted on a sensor node platform is dependent on the capabilities and constraints of sensor node hardware.

The Third Challenge:
Ad-hoc networking topology of WSN facilitates attackers for different types of link attacks ranging from passive eavesdropping to active interfering. Attacks on a WSN can come from all directions and target at any node leading to leaking of secret information, interfering message, impersonating nodes, etc.

The Fourth Challenge:
The communication in WSN is through wireless media, mainly radio. This characteristic of WSN makes wire-based security schemes impractical for WSNs.

The Fifth Challenge:
The topology of WSN is always dynamic. The sensor nodes can come and go in an arbitrary fashion. Node failures may be permanent or intermittent and this gives a higher level of system dynamics. Again very often large numbers of nodes are expected in sensor network deployments and the nature of this deployment is unpredictable.

The Sixth Challenge:
The overall cost of the WSN should be as low as possible.

KEY ISSUES FOR ACHIEVING THE SECURITY IN WIRELES SENSOR NETWORKS

Based on the analysis on security challenges and potential attacks on Wireless Sensor Networks, four key issues have been identified for providing security to the WSNs:

1) **Key Management in WSN:**
Confidentiality, integrity, and authentication services are critical factors for maintaining the security of a WSN. Key management is a highly important issue for this kind of protection in WSN. However, providing key management service in WSN is extremely difficult due to various constraints in the WSN environment, e.g., ad-hoc nature of the network, intermittent connectivity, resource limitation, limited communication bandwidth, etc.

2) **Encryption and Decryption Mechanism:**
Since the WSN environment is resource-constrained this encryption procedure as well as the decryption mechanism has to be very simple and energy efficient. Due to memory and energy constraints in a WSN environment we can not go for traditional asymmetric cryptography.

3) **Secure Routing of WSN:**
The major two types of threats in routing protocols of Wireless Sensor Networks are:
A) external attackers –
external attackers may become successful in partitioning a network or in introducing excessive traffic load into the network. Various attacks include: injection of erroneous routing information, replaying old routing information, distorting routing information, etc. Use of cryptographic schemes can defend against external attacks.
B) Internal compromised nodes –
it is difficult to put defense against such attacks. These nodes may send malicious information to other nodes in the network.

4) **Prevention of Denial-of- Service:**
A denial of service attack is any event that diminishes or eliminates a network's capacity to perform its expected function. Hardware failures, software bugs, resource exhaustion, environmental conditions, or any complicated interaction between these factors can cause a Denial-of-Service.

THREATS AT DIFFERENT LAYERS IN WIRELESS SENSOR NETWORK PROTOCOL STACK

We discuss different types of security threats present in different layers in the protocol stack of a Wireless Sensor Network. There are some types of security threats which span over more than one layer.

1) **Physical Layer:**

The communication media among the sensors is normally radio. Since the media is open there is a high risk present. Some of these threats are:

JAMMING

In this type of attack, adversaries interfere with the communication frequencies (radio frequencies) of the sensor nodes present in the network. For this purpose the adversary may select a few jamming nodes from within the network and then may apply jamming simultaneously from these selected nodes. In this case, the number of nodes the adversary

needs is a small fraction of the total number of nodes present in the network. Jamming is a popular Denial-of-Service (DoS) attack.

TAMPERING

In most of the applications, the number of sensor nodes deployed is very high and the geographic area over which those nodes are distributed is also very large. Therefore, it becomes impossible to control the access to all nodes from others. Again, the fabrication of the sensor nodes is simple and this is done mainly to reduce the cost. Normally tamper-resistant hardwares are not provided as it adds more cost to the sensor nodes. Due to these factors anybody can get access to the sensor nodes physically and even adversaries may introduce some identical sensor nodes into the sensor network field from their own side. Again, adversaries may become successful in compromising some of the legitimate nodes in the network. After compromising a node, adversaries may carry out lots of misleading activities inside the network.

SYBIL ATTACK

The base of Sybil Attack is actually at the physical layer but it becomes more prompt in the higher layers like link layer and network layer. In this class of attack, the adversary introduces a malicious node into the network. This can be done by compromising any legitimate sensor node or by fabricating a new node. This malicious node acquires identity through one of two ways: by fabricating new identities, or by stealing other identities. The malicious node behaves as if it were of different identities from different places in the network. It is a famous Classical Attack.

2) Data Link Layer:

Following are some of the security threats in link layer:

COLLISION

In this type of Denial-of-Service attack, adversary can induce collision in only one small portion of the entire packet transmitted by a node. A small change in the data portion of the packet leads to an error in the checksum of the whole packet and asks for retransmission of the same packet.

EXHAUSTION

Some link layer protocols attempt retransmission repeatedly, in the event of the transmission getting triggered by a collision. Adversaries may exploit it for doing exhaustive Denial-of-Service attack in which they continuously disturb the communication between two nodes and force the source node to retransmit continuously. This leads to quick decay in the energy level of the sensor nodes.

INTERROGATION ATTACK

Some Medium Access Control layer implementations use Request To Send (RTS) and Control To Send (CTS) packets to reserve channel access to transmit data. A malicious node can send RTS packets continuously to a targeted node by ignoring CTS reply packets. Then this can flood the network link of the targeted node. Normally, this type of attack is done by either a malicious node or by a self-sacrificing node.

SYBIL ATTACK

This type of attack is very much prominent in the Link Layer. Different variations of Sybil Attacks are as follows:

Data Aggregation:

Data aggregation is an important part in Wireless Sensor Networks as it reduces the power consumption as well as the bandwidth requirements for individual message transmission. In this situation, a Sybil Attack can be used to induce negative reinforcements. A single malicious node is sufficient to act as different Sybil Nodes and then this may give many negative reinforcements to make the aggregate message a false one.

Voting:

Voting may be a choice for a number of tasks in a Wireless Sensor Network. Many MAC protocols may go for voting for finding the better link for transmission from a pool of available links. Here, the Sybil Attack could be used to stuff the ballot box. An attacker may be able to determine the outcome of any voting and, of course, it depends on the number of identities the attacker owns.

3) Network Layer:

Major security goals of Network Layer are:

A. Every eligible receiver should receive all messages intended for it. Every receiving node should also be able to verify the integrity of every message as well as the identity of the sensor.

B. Routing protocol should also be responsible for preventing eavesdropping caused by misuse or abuse of the protocol itself.

In a Wireless Sensor Network, every node behaves as a router and routing issue is complicated from security point of view also. Designers of routing protocols did not consider security aspects during the design of the routing protocols and that is why Wireless Sensor Networks routing protocols are vulnerable to different types of attacks.

Here is a list of different types of attacks on the network layer:

NEGLECT AND GREED

In this type of attack a node that is present in the routing path can drop the message by participating in the lower level protocols. What the node does is send the "ACK" message of the link layer and drop the network layer message. The node can also give arbitrary priorities to the messages that pass through it.

MISDIRECTION

This is a more active attack in which a malicious node present in the routing path can send the packets in the wrong direction through which the destination is unreachable. In place of sending the packets in the correct direction, the attacker misdirects those and that too toward one node and thus this node may be victimized.

INTERNET SMURF ATTACK

In this type of attack, the adversary can flood the victim node's network link. The attacker forges the victim's address and broadcasts echoes in the network and also routes all the replies to the victim node. This way the attacker can flood the network link of the victim.

BLACK HOLE ATTACK

In this type of attack, some of the malicious nodes in the WSN intentionally advertise zero cost routes through them. Then some routing protocols (e.g., distance vector routing) establish a route to a destination by selecting this malicious node as an intermediate node into the routing path; (as they look for low cost link). Also the neighbors of this malicious node select this route and compete for the bandwidth. In this process the neighbors of this malicious node waste their energy and create a hole or partition in the network called a black hole.

SYBIL ATTACK

All multi-path routing protocols are vulnerable to Sybil attacks. The malicious node present in the network may advertise different identities. Then all paths in the multipath protocol may pass through the malicious node. And the protocol may have a picture of existence of different paths. But actually it is the same path through the malicious node. Sybil attack can actually fool the protocol giving a picture of existence of different routing paths to the destination but it is the same path through the Sybil node. On top of that even Geographic Routing Protocols are vulnerable to Sybil attack. It is because of the fact that the same Sybil Identity or different Sybil Nodes may give an illusion of their presence at different geographic locations.

SPOOFING AND ALTERING THE ROUTING INFORMATION

This is the most direct attack on a routing protocol because it targets the routing information which is exchanged between the nodes. By spoofing, altering, or replaying routing information, adversaries may be successful to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, and increase end-to-end latency.

WORM HOLE ATTACK

An adversary situated close to the base station may completely disrupt routing by creating a well-placed wormhole. An adversary could also convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. All existing routing protocols are vulnerable to this type of attack and there is no solid defense existing against the wormhole attack.

SELECTIVE FORWARDING ATTACK

Normally it is believed that in a multihop network, participating nodes will faithfully forward the received messages. But sometimes this does not happen. This is what exactly happens in a selective forwarding attack – malicious nodes may refuse to forward certain messages and they drop these messages to ensure that the messages do not get propagated further. A simple form of this attack is a malicious node behaves like a black hole and does not forward every packet it receives. But

such an attacker may fail because the neighboring nodes may conclude that it has failed and decide to seek another route.

Another form of this attack is:
an adversary may selectively forward packets. Here the adversary may be interested in suppressing or modifying packets originating from a few selected nodes. In this situation, the adversary reliably forwards the remaining traffic to limit the suspicion of wrong-doing.

HELLO FLOOD ATTACK
Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors. A node receiving such a packet may assume that it is within radio range of the sender. And this assumption may be false.

4) Transport Layer:

Different types of threats present in the Transport Layer are as follows:

FLOODING ATTACK
Protocols that maintain state information at either end of the communication are vulnerable to flooding attack. One well-known attack is TCP SYN flood attack in which the adversary continuously sends the connection requests and floods the network link at the targeted node.

DE-SYNCHRONIZATION
By disrupting some of the packets transmitting in between the nodes and by maintaining proper timings, an adversary can make a pair of nodes stuck in synchronization recovery protocol. This compels the nodes to waste their energy.

SOLUTIONS AT DIFFERENT LAYERS IN WIRELESS SENSOR NETWORKS

1. Physical Layer:

JAMMING
Various forms of spread-spectrum communication are used as defense against Jamming. Frequency hopping is one form of spread-spectrum approach and this has been widely used as a defense against Jamming. In this approach, all communication nodes maintain a hopping sequence. Here the tricky point is, a jammer can get the hopping sequence if he observes the transmission and therefore hopping should be done very fast. In that case the jammer cannot interfere with the communication. The cost involved against frequency hopping is higher as the sensor nodes re power constrained as well as have low computational capability.

TAMPERING
The defense mechanism designed against tampering should prevent the attackers (adversaries) from getting any information about cryptographic keys or about the network, even though it is successful in compromising some of the nodes. Here is a list of few *defenses:*

1) Self Destruction –
whenever somebody accesses the sensor nodes physically the nodes vaporize their memory contents and this prevents any leakage of information.

2) Fault Tolerant Protocols –
the protocols designed for a WSN should be resilient to this type of attack. This means even if some nodes are removed from the network setting or they are compromised, still the network should function properly.

SYBIL ATTACK
Normally this class of attack is tackled efficiently in the higher layers of the protocol stack in a WSN, though they originate in the physical layer only. Some preventive measures like fixing of the number of nodes in a WSN (which may depend on the type of application the WSN is intended for) can be taken which will prevent the adversary from fabricating new identities.

2. Link Layer:

Good encryption mechanism, authentication mechanism, and error correcting techniques are required to put defense against most of the link layer threats. Since the sensor nodes are resource constrained, the above-mentioned techniques should not be computation intensive and they should not put much overhead to the sensor nodes and also communication overhead should be minimum.

COLLISION
Providing error correcting codes – error correcting codes can be incorporated in the data packets to defend against collision. But this solution comes at a higher cost in terms of computational complexity and energy consumption.

EXHAUSTION
The defense against exhaustive Denial-of-Service attack is very simple and still effective. If a node retransmits a message for more than a threshold number of times, then the node identifies itself as under attack and goes to sleep mode. Later it may be awakened and resume its normal operation.

INTERROGATION ATTACK
To put a defense against such type of attacks, a node can limit itself in accepting connections from same identity. During implementation, it may be decided that a particular node will not accept more than a fixed number of connections from the same identity. A careful selection has to be made in fixing this threshold value.

SYBIL ATTACKS
Radio Resource Testing – It is a popular defense against Sybil Attack. If one node is interested in verifying whether its neighbors are valid or Sybil identities, then this node can assign each of its "n" neighbors a different channel to broadcast some test messages. After this, the node can listen to any channel and find out whether the neighbor that was assigned that channel is legitimate. Apart from this, some secret information may be shared by a node with its neighbors and Sybil identities may be detected. But this may put some extra communication overhead.

3. Network Layer:

The problem of securing the network layer reduces to the problem of securing route discovery of a routing protocol.

NEGLECT AND GREED AND SELECTIVE FORWARDING ATTACK
One simple defense against this type of attack is: use multiple routing paths or send redundant messages (which is, of course, not a power efficient scheme), through which the probability of selecting a vulnerable route can be reduced. This can also force the adversary to compromise more nodes to succeed.

MISDIRECTION AND INTERNET SMURF ATTACK
This kind of attack can be handled easily as follows: If it gets observed that a node's network link is flooded without any useful information, then the victim node can be scheduled into sleep mode for sometime.

BLACKHOLE ATTACK
This type of attack can be defended by accepting routing replies only from authorized nodes. Unauthorized nodes can easily be identified by just checking if some node is behaving abnormally.

SYBIL ATTACK
There is no effective defensive mechanism available against Sybil attack in Network Layer. But it is important to note that this attack cannot survive only in routing layer. First, the attacker interested in Sybil attack must attack the link layer and also get Sybil identities. And very good defensive mechanisms for Sybil attack in link layer are available through which this type of attack can be defended in the link layer itself.

RUSHING ATTACK
One defense against rushing attack is by detecting a secure neighbor. And this may be done by bi-directional checking of the link while electing the route.

WORMHOLE ATTACK AND HELLO FLOOD ATTACK
One defense against these types of attacks are by checking the bi-directional link whenever selecting a path.

Again location-based routing protocols can avoid wormhole attacks since, in these protocols, each node knows approximately how many hops it is from sink. Here, wormholes cannot fool the nodes since they know their location.

SPOOFING, ALTERING MESSAGES
Efficient encryption and authentication techniques can defend atainst spoofing attacks. Encryption may be applied to some required fields in the header of the message. This may save some energy from computing and communicating some extra bits. TESLA can be adopted for authentication.

4. Transport Layer:

The security issues in the transport layer are mainly due to the existence of the flaws in the transport layer protocols. Efficient design of

transport layer protocols can avoid transport layer threats.

FLOODING ATTACKS

As a defense against this class of attack, a limit can be put on the number of connections from a particular node. Again, a careful selection has to be made in determining this upper limit on the number of connections. A study of the topology of the network may be helpful in this regard.

DESYNCHRONIZATION

A solid authentication mechanism can be deployed to authenticate all packets exchanged, including all control fields in the transport packet header. It is assumed that the authentication mechanism is robust and adversaries also cannot forge this mechanism. In this situation, the end nodes can detect malicious packets and ignore same.

CONCLUSION AND FUTURE SCOPE

Providing security in Wireless Sensor Network is a non-trivial task. Herein, we have studied different key issues in achieving security in WSN. We have also studied different threats existing in different layers of the protocol stack of WSN. Possible solutions against different threats have also been outlined. This work was undertaken by the authors and is in progress regarding the design of a security framework for wireless sensor networks. The mathematical modeling of different threats present in the WSN is another aspect of this work.

ACKNOWLEDGEMENT

The authors are grateful to Prof. Rajib Mall, Department of CSE IITKGP, India, for his constant support and guidance.

REFERENCES

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, A survey on sensor networks, *IEEE Communications Magazine*, 40(8): 102-114, August 2002.

[2] Feng Zhao and Leonidas Guibas, *Wireless Sensor Networks an information processing approach*, Elsevier ISBN: 81-8147-642-5.

[3] William Stallings, *Cryptography and Network Security Principles and Practices, Third Edition*, Pearson Education. ISBN 81-7808-902-5.

[4] A. Asokan and P. Ginzboorg, Key Agreement in ad-hoc networks, *Computer Communications*, 23: 1627-1637, 2000.

[5] Adrian Perrig, John Stankovic and David Wagner, Security in Wireless Sensor Networks, *Communications of the ACM, June 2004/Vol. 47, No. 6.*

[6] Chennakesavulu V., B. Dey and S Nandi, Securing Wireless Sensor Networks: Challenges in Different Layers and Possible Solutions, *Proceedings of National Workshop on Trends in Advanced Computing NWTAC 2006*, pp. 73-82.

[7] Fei Hu, Jim Ziobro, Jason Tillett, Neeraj and K. Sharma, Secure Wireless Sensor Networks: Problems and Solutions, internet draft.

[8] C Karlof and D Wagner, Secure Routing in Wireless Sensor Networks: Attacks and Countemeasures, *Sensor Network Protocols and Applications (SNPA 2003)*, May 2003.