SECURITY ANALYSIS OF WIRELESS SENSOR NETWORKS

Rajni Sharma*

Chander Diwakar**

ABSTRACT

Wireless sensor network have great potential to be employed in various situations and applications. Originating from military research projects, WSNs are expected to be used in more civil applications. Wireless sensor network faces the challenge to securely sense the physical environment, process the sensed data collectively and securely communicate among nodes. All this based on trust among the nodes. The security threats of WSN comes not only from the external attacker but also from the internal node misbehavior. Misbehavior of nodes may range from simple selfishness or lack of collaboration due to the need for power saving to active attacks. Cryptography & authentication only suitable for external attacks. This paper discusses a wide variety of attacks in WSN, cryptography attacks, trust based routing methods, key management and dynamic host configuration in WSN.

Keywords*: Wireless Sensor Network, Attacks, Key Management, Cryptography Attacks.*

*University Institute of Engineering and Technology, Kurukshera University, Kurukshera.

**Lecturer, University Institute of Engineering and Technology, Kurukshera University, Kurukshera.

1. INTRODUCTION

In computer networking there is a great value of wireless networking because it can be easily installed, less expenditure and has various way to save money or band time. Wireless sensor networking is another form of networking in the field of wireless networking. Wireless sensor network comprised on number of numerous sensors which are interlinked or connected with each other for performing the same function collectively or cooperatively in order to check and balance the environmental factors. This type of networking is called as Wireless sensor networking. Basically in wireless sensor networks the physical conditions such as weather conditions, regularity of temperature, different kinds of vibrations are monitored and also deals in the field of technology related to sound. Sometimes it is also used in pressure, and also checking the environmental pollutants.

These sensors are distributed spatially which are used collectively for performing a function other wise it is difficult for the sensors to perform cooperatively to play a role in monitoring. Wireless sensor networks play a vital role in battle field surveillance which is completely a military application. It is also play an important part in applications like monitoring of traffic control and many others. The main characteristics of a WSN include Power consumption constrains for nodes using batteries or energy harvesting, Ability to cope with node failures, Mobility of nodes, Dynamic network topology, Communication failures, Heterogeneity of nodes, Scalability to large scale of deployment, Ability to withstand harsh environmental conditions, Ease of use, Unattended operation and Power consumption. WSNs can be used in large number of different applications. Originating from military research projects, WSNs are expected to be used in more civil applications. In testbeds, a variety of different application scenarios for WSNs have been investigated, e.g.: habitat monitoring, emergency response, glacier surveillance, volcano surveillance, wildlife monitoring, Marathon Net, traffic monitoring , surveillance missions, structural monitoring, vehicle tracking and mobile counter sniper system

1.1 The differences between wireless sensor networks and ad hoc networks

WSN differ in many fundamental ways from MANETS as mentioned (1) Sensor networks are mainly used to collect information from sensor nodes while MANETS are designed for distributed computing rather than information gathering. (2) Sensor nodes mainly use broadcast communication paradigm whereas most MANETS are based on point-to-point communications. (3) The number of nodes in sensor networks can be several orders of magnitude higher than that in MANETS.(4) Sensor nodes may not have global identification

(ID) because of the large amount of overhead and large number of sensors whereas nodes in MANET may have global Identification.(5) Sensor nodes are much cheaper than nodes used in a MANET and are usually deployed in thousands. (6) Sensor nodes are limited in power, computational capacities, and memory where as nodes in a MANET can be rechargeable somehow. (7) Usually, sensors are deployed once in their lifetime, while nodes in MANET really in an Ad-hoc manner. (8) Sensor nodes are much more limited in their computation and communication capabilities than their MANET counterparts due to their low cost. Special Issue on Ubiquitous Computing Security Systems

2. SECURITY IN WIRELESS SENSOR NETWORK

The first challenges of security in sensor networks lie in the conflicting interest between minimizing resource consumption and maximizing security. Major resource constraints into consideration: (1) limited energy (2) limited memory (3) limited computing power
(4) limited communication bandwidth (5) limited communication range

2.1 Security Goals

(1) **Availability:** Network resources should be available to authorized nodes when needed and the sensor network should ensure the survivability of network services despite denial of a service (DoS) attack.

(2) **Data Integrity**: It ensures that the received data is not altered or destroyed in transit by an adversary.

(3) **Authenticity:** An adversary might easily inject fake messages, so the receiver needs to make sure that the data originates from a trusted source.

(4) **Scalability:** Sensor networks can not utilize a keying scheme that has poor scaling properties in terms of energy cost or latency. In general, the number of neighbors and the distance or power required to send messages from one node to another will not be known in advance.

(5) **Confidentiality:** A confidential message is resistant to revealing its meaning to an eavesdropper. Confidentiality should be provided by keys such as public key or private key.

(6) **Freshness:** It implies that the data is Fresh and also ensures no adversary has replayed old messages.[2]

2.2 Various attacks in WSN

Wireless Sensor networks are threatened to security attacks due to the broadcast nature of the transmission medium as well as nodes are often placed in an unfriendly or dangerous environment, where they are not physically protected. Two main types of attacks:

(a) **Passive attacks** (b) **Active attacks**

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	Wormhole, blackhole, Byzantine, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

Table 2.1 Security Attacks on Each Layer of the Internet Model

Cryptographic Primitive Attacks	Examples
Pseudorandom number attack	Nonce, timestamp, initialization vector (IV)
Digital signature attack	RSA signature, ElGamal signature, digital signature standard (DSS)
Hash collision attack	SHA-0, MD4, MD5, HAVAL-128, RIPEMD

Table 2.2 Cryptographic Primitive Attacks

A. Passive Attacks[3]

In this attack selfish nodes use the network but do not cooperate, saving battery life for their own communications; they do not intend to directly damage other nodes.

Attacks against Privacy*:* Much information from sensor networks could probably be collected through direct site observation. But sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Hence, adversaries need not be physically present to maintain observation.

- **Monitor and Eavesdropping:** By snooping to the data, the adversary could easily discover the communication data. The control packets conveyed by network about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection.

- **Traffic Analysis:** Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network by analysis of communication patterns.[3]
- **Camouflage Adversaries:** A malicious node can be inserted as normal node and than these nodes act as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis.

B. Active Attacks

In this attack malicious nodes damage other nodes by causing network outage by partitioning, while saving battery life is not a priority. Various types of active attacks are:

1. Routing Attacks in Sensor Networks
2. Denial of Service Attacks
3. Node Subversion
4. Node Malfunction
5. Node Outage
6. Physical Attacks
7. Message Corruption
8. False Node
9. Node Replication Attacks
10. Passive Information Gathering

1) Routing Attacks in Sensor Networks [5]

The attacks working at network layer are called routing attacks. Various routing layer attacks at network layer are

a) Spoofed, altered and replayed routing information

An unprotected adhoc network invites various attacks at network layer such as Creation of routing loops, Extend or shorten service routes, Generate false error messages, Increase end-to-end latency.

b) Selective Forwarding

An adversary can selectively drop some packets. It is necessary that nodes faithfully forward and receive every messages in sensor networks but some malicious nodes deny to forward packets, so nodes looking for new routes.[8]

c) Sinkhole Attack

In sinkhole attack the aim of adversary is to attract all the nearby traffic from a particular region through a malicious node. Attracting network traffic to a specific (compromised) node in called sinkhole attack.[12]

d) Sybil Attacks

In sybil attack a single node presented itself as multiple nodes in the multiple locations. It mostly targets fault tolerant schemes such as distributed storage, multipath routing and

topology maintenance. Authentication and encryption techniques can be used to prevent sybil attack to be launched by an outsider in the sensor network[12]

e) Wormholes Attacks:

In this case, an attacker node receives packet at one location in the network and tunnels them to another location in the network, where these packets are resent into the network. This tunnel between two malicious nodes is called wormhole. No harm is done if the wormhole is used properly for efficient relaying of packets, it put the attacker in a powerful position in the network and it could compromise with the security of network

f) HELLO flood attacks

In this type of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a large number of sensor nodes that are isolated in a large area within a WSN. The sensors are thus influenced that the adversary is their neighbor. So while sending the information to the base station, the target nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.[5]

2) Denial of Service

In this case, an adversary attempt to prevent legitimate and authorized users of network in accessing services offered by the network .DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed.[4]

Layer name	***Type of DoS Attack***
Physical layer	Jamming, tampering
Data link layer	collision, exhaustion and unfairness,
Network layer	neglect and greed, homing, misdirection, black holes
Transport layer	malicious flooding and de-synchronization
Application layer	Malicious programs can cause DoS attacks

Table 2.3: Various Dos attacks

3) Node Subversion

An adversary can capture a sensor node, which may reveal its information including disclosure of cryptographic keys and thus affect the whole sensor network.

4) Node Malfunction

If a node starts malfunctioning, it will generate erroneous data that could expose the integrity of sensor network. Especially if malfunctioning node is a data-aggregating node such as a cluster leader will lead to more damage to network.

5) Node Outage

It is the situation which occurs when a node stops working. In the case where a cluster leader stops functioning, in order to mitigate the effects of node outages the sensor network protocols should be robust enough to provide an alternate route [9]

6) Physical Attacks

Sensor networks typically operate in hostile environments which make them highly susceptible to physical attacks, such as threats due to permanent physical node destructions. An attackers can also extract cryptographic secrets(keys), tampering associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.[5]

7) Message Corruption

Any modification with the contents of a network message by an attacker compromises its integrity.

8) False Node

A false node injection by an adversary can causes the injection of malicious data. Malicious code injected in the network, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary.[4]

9) Node Replication Attacks

In this attack, an attacker seeks to add a new node to an existing sensor network by copying the existing sensor node ID. This false node can corrupt the Packets or even misroute them. This can result in a disconnected network, false sensor readings, etc. If an attacker can gain physical access to the entire network he can copy cryptographic keys to the replicated sensor nodes. By inserting the replicated nodes at specific network points, the attacker could easily manipulate a specific segment of the network, perhaps by disconnecting it altogether.[14]

10) Passive Information Gathering

An adversary with powerful resources can collect information from the sensor networks if it is not encrypted.. Interception of the messages containing the physical locations of sensor nodes, message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.

2.3 Cryptographic primitive attacks

Weakness in security protocols leads to security holes. Malicious attacks often target authentication protocols and key exchange protocols. Cryptographic primitives are considered to be secure but some problems are discovered. Some cryptographic primitive attacks are discussed as following.

A. Pseudorandom number attacks*:*

A timestamp or random number is used to make data/control packets fresh in order to prevent a replay attack. In the public key infrastructure the shared secret key and the session key is often generated from a random number. In the best case, random numbers are generated based on physical sources of randomness that cannot be predicted such as noise from an electronic device or the position of a pointer device is a source of such randomness. Pseudorandom numbers must be used on the non availability of physical randomness.

B. *Digital signature attacks:* [8]

Digital signature can be generated using the RSA public key algorithm. But it suffers from one problem: that is blind signature attack. The user can get the signature of a message and use the signature and the message to fake another message's signature. Various digital signature attack models can be classified into known-message, chosen-message, and key- only attacks.

In the **known message attack**, the attacker knows a list of messages previously signed by the victim.

In the **chosen-message attack**, the attacker can choose a specific message that it wants the victim to sign.

Whereas in the **key-only attack**, the adversary only knows the verification algorithm, which is public.

C. Hash collision attacks:

The goal of a collision attack is to find two messages with the same hash, but the attacker cannot pick what the hash will be. Generally all major digital signature techniques (including DSA and RSA) involve two processes first hashing the data and then signing the hash value. The digital signature algorithm does not sign the original message data directly, for both performance and security reasons. Collision attacks could be used to tamper with existing certificates. An adversary might be able to construct a valid certificate corresponding to the hash collision.[9]

D. Key management vulnerability:

Key management protocols used for the key generation, storage, distribution, updating, revocation, and certificate service. Attackers can launch attacks to disclose the cryptographic key at the local host or during the key distribution procedure. The lack of a central trusted entity in WSN makes it more vulnerable to key management attacks.

2.4 Trust Based Routing Methods

Enhancements in the routing related protocols based on the trust have been widely addressed in the literature.

A. **ARIADNE:[18]** It is very efficient protocol, using highly efficient symmetric cryptographic primitives and per-hop hashing function. It prevents the attackers or compromised nodes from tampering with uncompromised routes consisting of uncompromised nodes, and also prevents a large number of types of Denial-of-Service attacks.

B. **ATSR** (Ambient Trust Sensor Routing): A fully distributed Trust Management System is realized in ATSR in order to evaluate the reliability of the nodes. Different trust metrics are used to find the direct trust value per neighbor of nodes by monitoring the behavior of their neighbors.

C. **Trusted AODV:** In this routing protocol trust metrics are used to perform secure routing. First, a trust based recommendation mechanism introduced and depending on this trust recommendation the routing decision rules of AODV are modified

D. **Trusted GPSR:** The Greedy Perimeter Stateless Routing [6] is modified to take trust levels of node into account. A node maintains a trust value for its neighbors when each time it sends out a packet and waits until it overhears its neighboring node forwarding it. Based on this correct and prompt forwarding information routing decisions are made.

E. **SPINS[19]:** SPIN provide trusted routing but it does not support Denial of service attack. This routing protocol has been designed to provide data authentication, data confidentiality and evidence of data freshness. Two security blocks SNEP and μTESLA are introduced in this protocol. The first block SNEP introduces overhead of 8 bytes and maintains a counter fro achieving semantic security. μTESLA provides authentication for data broadcasting.

F. **Trust-aware DSR:** In the Dynamic Source Routing protocol, the watchdog and Pathrater modules has been designed and integrated for security. The watchdog module detects selfish nodes that do not forward packets. For this, each node in the

network buffers every transmitted packet for a limited period. In order to overhear whether the next node has forwarded the packet or not, each node enters into promiscuous mode during this period.

G. **CONFIDANT:** (Cooperation of Nodes, Fairness In Dynamic Adhoc Networks) CONFIDANT adds reputation system and a trust manager to the Watchdog and Pathrater scheme. The events reported by the Watchdog are evaluated by the trust manager and issues signals to other nodes regarding malicious nodes. The signal recipients are maintained in a friends-list. The reputation system maintains and shares a black- list of nodes at each node with the friends-list nodes.

H. **TRANS:** This routing protocol selects routes based on trust information from the network rather than on hop count to avoid the insecure locations. It is assumed that the sensors know their geographical locations and that geographic routing is possible. A sink sends a message only to its trusted neighbors for the destination location. Neighbor Nodes that have the nearest location to destination forward the packet to their trusted neighbors. Thus the packet reaches the destination along a path of trusted sensors.

2.5 Dynamic Host configuration/address auto configuration in wireless sensor network

In WSN logical resources such as naming, addressing and topology control must be organized and controlled as the .physical resources such as memory, processing power and energy are. Wireless sensor networks do not support fixed addressing of nodes because the applications in WSN itself does not require globally unique addresses. The deployment and maintenance of wireless sensor networks becomes much easier if address-less or data-centric operations are enabled. Nodes can be deployed (or replaced) without changing the node programme.[16]. The overhead required for global dynamic address assignment is too much high. Some prominent solutions are gossiping and flooding in data centric routing approaches. Geographical routing is also an address less routing.

DHCP(Dynamic Host Configuration Protocol): DHCP (Droms, 1997, 2004) is a client-server-based network protocol[16]. This protocol is based on two major building blocks: a protocol for delivering specific parameters to the client and a mechanism for selection and suggesting IP addresses. Each DHCP server maintains several address pools that hold information about available and currently used addresses. The address management is server-oriented. DHCP supports three different mechanisms for IP address allocation: **automated, operator-controlled and dynamic**. In automated mechanism IP addresses are permanently assigned to clients after their first registration. Whereas, an operator can

manually assign an address to a particular client in operator controlled mechanism. Finally, in dynamic address allocation have possibility to temporally assign an IP address to a client. This assignment of particular address to a node is in the form of a lease, for a stipulated period. When the lease period of node ends the entire process is renewed and the same or a new IP address is issued again to the node. When a node is no longer in need of an IP address, it informs the DHCP server which in turn pools the IP into its resource for future use. With the help of dynamic assignment the addresses can be reused after the first allocation. Thus, dynamic address allocation is usually used if only short-term connections of clients are envisioned. Focusing on the management and control in ad hoc and sensor networks, this seems to be an adequate solution[16]. Unfortunately, all the assignments are based on the MAC address of each client that is worldwide unique. Therefore, DHCP only maintains an IP address to MAC address binding.

2.6 Key management in WSN

Security in WSN requires node-to-node secure communication by key mechanism, which includes both data encryption and authentication. Since resources are limited in WSN, traditional key management schemes such as trusted third party like KDC (key distribution center) and asymmetric key cryptography are not suitable for WSN. It was due to the resource constraints of sensor nodes that always lightweight key management schemes proposed for wireless sensor networks. So maintaining required level of security in wireless sensor networks is also very important. Various key management techniques are Single Network-Wide Key, Pairwise Key Establishment Scheme, Random Key Predistribution.

3. CONCLUSION

Security in Wireless Sensor Network is vital to the acceptance and use of sensor networks. In this paper, we have made a security analysis to the Wireless Sensor Network and also gone through key management and secure routing techniques. Encryption and authentication only prevent from outside attackers. But useless in case of internal malicious node attacks. DHCP concept is also discussed to uniquely identify nodes

4. REFERENCES

1. Anthony D. Wood and John A. Stankovic, “A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks”
2. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, “Security in Wireless Sensor Networks: Issues and Challenges”, pg 1043-1048 Feb. 20-22, 2006 ICACT2006

3. Fei Hu, Jim Ziobro, Jason Tillett, Neeraj K. Sharma, "Secure Wireless Sensor Networks: Problems and Solutions" SYSTEMICS, CYBERNETICS AND INFORMATICS VOLUME 1 - NUMBER 4
4. Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009
5. TEODOR-GRIGORE LUPU, "Main Types of Attacks in Wireless Sensor Networks" Recent Advances in Signals and Systems"
6. Khairul Azmi Abu Bakar and James Irvine, "A Scheme for Detecting Selfish Nodes in MANETs using OMNET++", 2010 Sixth International Conference on Wireless and Mobile Communications 978-0-7695-4182-2/10 $26.00 © 2010 IEEE, DOI 10.1109/ICWMC.2010.14
7. Qun Liu, Xingping Xian, Songtao Guo, Tao Wu, "Research on Cooperative Packet Forwarding and Punishment Mechanism in Wireless Sensor Networks" 2010 IEEE International Conference on Granular Computing
8. Atul kahate , "Cryptography And Network Security" 3rd edition
9. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003
10. I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communication Magazine, Aug. 2002.
11. F. Hu and N. K. sharma. Security considerations in ad hoc sensor networks. Ad Hoc Networks (Elsevier), 3(1):12–23, August 2005.
12. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", AdHoc Networks (elsevier), Page: 299-302, year 2003
13. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges**",** International conference on Advanced Computing Technologies**,** Page1043-1045, year 2006
14. Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004
15. Al Sakib Khan Pathan , "Security_of_Self_Organizing Networks, MANET, WSN, WMN, VANET"
16. Dressler, F. and Chen, F. (2007) 'Dynamic address allocation for self-organised management and control in sensor networks', *Int. J. Mobile Network Design and Innovation*, Vol. 2, No. 2, pp.116–124.

17. Dr. Eric Cole, "Swarm Intelligence and Network Administration: Applications in Ad Hoc Wireless Auto-Configuration"
18. Y. C. Hu, A. Perrig and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Net- works," Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, Atlanta, 23-28 September 2002, pp. 12-23. doi:10.1145/570645.570648
19. Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victorwen and David E. Culler, "SPINS: Security Protocols for Sensor Networks", ACM Journal of Wireless Networks, 8:5, September 2002, pp. 521 – 534