Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 4, April 2016, pg.170 – 177

WIRELESS SENSOR NETWORK SECURITY – AN ANALYTICAL SURVEY

Suchithra[1], Sumitha Thankachan[2]
[1]Graduate Trainee, Academic Coordinator Office, Amrita Vishwa Vidyapeetham(ASE), Coimbatore, India
[2]Assistant Professor, Department of Computer Science, BVM Holy Cross College, Cherpunkal, Kerala, India
chanu.suchithra@gmail.com
sumitha.thankachan@gmail.com

Abstract*— The researchers are facing numerous unique challenges with the emergence of the sensor networks which is posing as one of the dominant technology trend in the current decade. The sensor networks which are likely composed of hundreds, and potentially thousands of tiny sensor nodes, function autonomous, in many cases, without the access to the renewable energy resources. Some important factors such as cost constraints, need for ubiquitous and invisible deployments will also result in the small sized, resource-constrained sensor nodes. In this paper, we concentrate on the security of Wireless Sensor Networks, since the set of challenges in the sensor networks are much diverse in nature. We have made a depth threat analysis of Wireless Sensor Network and also propose some of the countermeasures against these threats. We also propose some of the security goals for the Wireless Sensor Network. In further, security is more important for the acceptance and the usage of the sensor networks for as many applications.

***Keywords*— Wireless Sensor Network (WSN), Security.**

I. INTRODUCTION

The term sensor network is used to refer a heterogeneous system which combines one or more sensors and actuators with the purpose of computing elements. The Applicative domain of the Wireless Sensor Network are vast diverse which is due to the availability of more number of micro-sensors and low-power wireless communications. In the remote sensor network, unlike the traditional sensors, a vast number of sensors are densely deployed. These sensor nodes perform high significant signal processing, computational intelligence works i.e., adding and dropping, and network self-configuration to achieve more functional & non-functional properties such as scalability, robustness and long-lived networks[5]. Much specifically, the sensor nodes will be doing local processing for reducing communications, and subsequently, energy costs. We also believe that the most efficient and adaptive routing model for WSN is a cluster based hierarchical model. In a cluster based wireless sensor network, the cluster formation in a network plays a key factor in the cost reduction, here cost refers the expense of the wireless setup and the maintenance of the sensor networks.
In this paper, we explore a more in-depth look of security in WSN and also have a discussion on its counter measures.

© 2016, IJCSMC All Rights Reserved

II. ARCHITECTURE OF A WIRLESS SENSOR NETWORK

A typical WSN consists of the following network components:

- **Sensor motes (Field devices)** – The field devices which are mounted in the process, must be capable of routing the packets on the behalf of other devices in the network. In most of the cases, the characterization or the control of the process or the process equipment is quite entrepreneurial. A router is a special type of field device which do not have any process sensors or the control equipment, which controls the network access and it also does not have the interface with the process itself.
- **Gateway or Access points** – A Gateway enables the communication between the host application and the field devices.
- **A Network manager** – A Network Manager is the one which is responsible for the configuration of the network. It also schedules the communication between the devices (i.e., configuring super frames), helps in the management of routing the tables and also helps in monitoring and reporting the current status of the network.
- **The Security manager** – The Security Manager does Key generation, Key storage, and Key management.

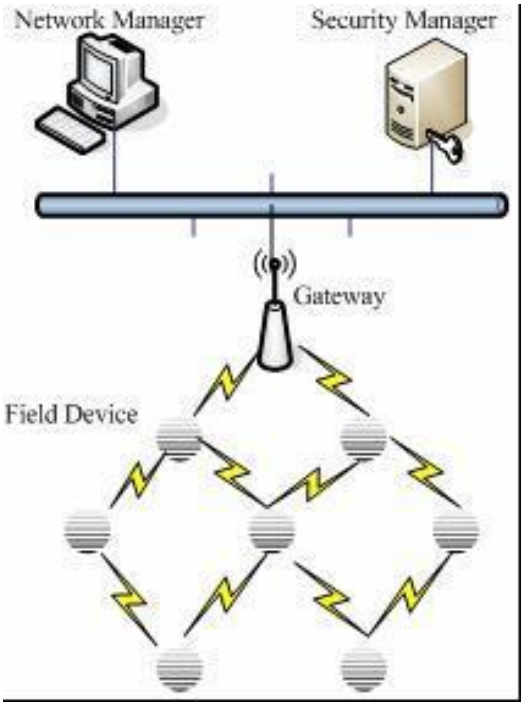

Fig. 1. WSN Architecture

III. SECURITY ANALYSIS OF A WSN NETWORK

The simplicity in Wireless Sensor Network is with the resource constrained nodes which makes them extremely vulnerable to a variety of attacks. Attackers can eavesdrop on the highly confidential transmission, add/drop bits to the channel, replay the previously send packets and many more attacks. The Security of the Wireless Sensor Network supports all the functional and non-functional security properties: confidentiality, integrity, authenticity and availability. Attackers deploy malicious nodes with the similar hardware capabilities in which the legitimate nodes collide to attack the system cooperatively. The attacker might come upon purchasing these malicious nodes separately, or by "turning" a few legitimate nodes by capturing and physically overwriting the memory of the nodes. In some cases, colliding nodes may have high-quality communicative links which are available for the coordination of the attack. Sensor nodes are not tamper resistant and if there is any resistance nodes which adversary compromise any node, then the attacker can extract all the key material, data, and code which is stored on that particular node. While the tamper resistance may be viable defense for the physical node compromise for some wireless networks, where we do not see the presence of any general purpose solution. In extreme

© 2016, IJCSMC All Rights Reserved

cases, an effective tamper resistance also tend to add a significant rate of per-unit cost, and the sensor nodes are intended to be a very inexpensive [1] [2] [3] [4] to afford.

The identification and categorization of attacks in a Wireless Sensor Network is as follows:

3.1. Denial of Service Attack

Denial of Service (DoS) is an event which occurs and diminishes or eliminates the performance capacity of the network and its expected function [16].

Different Types of DoS Attacks:

There are 12 different DoS Attacks in different Layers of Interconnects:

Attack 3.1.1 DoS/Physical Layer Attack/Jamming - To attack a node or a set of nodes, a simple transmission of a signal which interferes the frequencies that is being used by the sensor network. Interrupting the channel with an unwanted signal.

Attack 3.1.2 DoS/Physical Layer Attack/Tampering/Physical Tampering - Nodes are vulnerable to physical harm, or tampering (i.e. reverse engineering).

Attack 3.1.3 DoS/Data Link Layer/Collision.

Attack 3.1.4 DoS/Data Link Layer/Exhaustion.

Attack 3.1.5 DoS/Data Link Layer/Unfairness.

Attack 3.1.6 DoS/Network Layer/Neglect and Greed.

Attack 3.1.7 DoS/Network Layer/Homing.

Attack 3.1.8 DoS/Network Layer/Spoofing. Misdirection. In this type of attack adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc.

Attack 3.1.9 DoS/Network Layer/Black Holes.

Attack 3.1.10 DoS/Network Layer/Flooding.

Attack 3.1.11 DoS/Transport Layer/Flooding.

Attack 3.1.12 DoS/Transport Layer/De-synchronization.

3.2. Interrogation

Attack 3.2.1 Interruption/Data Link Layer.

3.3. Sybil Attack in Wireless Networks

A malicious device illegitimately taking multiple identities is called Sybil Attack. Sybil attack [7], is used as an adversary which can be found in more than one place at a time as a single node that presents multiple identifications to other nodes in the wireless network that can also significantly be helpful in the reduction of the effectiveness of the fault tolerance schemes. For example: Distributed storage [8], dispersity [9] and Multipathing. It is extremely difficult for an adversary for launching an attack in the network where every pair of neighboring nodes uses an unique key for initializing the frequency hopping or the spread spectrum technologies in communication. One of the geographic routing protocol threat is sybil attack.

Types of Sybil Attacks in the Communication Interconnect:

Attack 3.3.1 Sybil/Physical Layer.

Attack 3.3.2 Sybil/Data Link Layer/Data Aggregation.

© 2016, IJCSMC All Rights Reserved

Attack 3.3.3 Sybil/Data Link Layer/Voting.

Attack 3.3.4 Sybil/Network Layer.

3.4. Wormhole Attack

A wormhole attack [10], is an adversary tunneling of messages that are received in the part of the network over a low latency link which replays them at a different part. An unauthorized node is situated close to the base station where they are completely disrupted and routed by creating a well-placed wormhole. An unauthorized node could convince other nodes who would normally be multiple hops from the base station from one or two hops away via the wormhole. This process can create a sinkhole: where the unauthorized node on the other side of the wormhole artificially provides a high-quality route to the base station, where it potentially stop all traffic in the surrounding area where alternate routes are significantly less attractive and powerful.

Attack 3.4.1 Wormhole/Network Layer. For example: A routing attack is possible in an adversary network node of a shorter, or zero, path to the base station which can disrupt the network.

3.5. Black hole Attack

Blackhole attacks are typically done by making a compromised node look attractive to the surrounding nodes with respect to the routing algorithm that is employed in the communicative network which lures all the traffic from a particular area through a compromised node, by creating a metaskeptical sinkhole with the adversary at the center.

Attack 3.5.1 Sinkhole/Network Layer.

3.6. Manipulating Routing Information

Attack 3.6.1 Manipulating Routing Information/Network Layer.

3.7. Selective Forwarding Attack

A selective forwarding attack, do have a malicious nodes which behaves like a black hole and do refuse to send messages and drop them, assuring that the sent messges have not propagated any further. In some cases, an attacker can run the risks where the neighboring nodes would conclude that the sender has failed to seek another route.

Attack 3.7.1 Selective Forwarding/Network Layer.

3.8. Hello Flood Attack

Many protocols employed in network security require nodes to be broadcasted HELLO packets to announce them to their neighbors, A neighbor node may send HELLO to other nodes but this may even cause a flood of packets to be transferred along with the data packets. This usually happens interrupts the working of the network layer.

Attack 3.8.1 Hello Flood/Network Layer.

3.9. Acknowledgement Spoofing Attack

Network routing algorithms rely on implicit or explicit link layer acknowledgements. The receiving end of the network usually acknowledges the sender regarding the receiving of the packets. But too much acknowledgement messages from th receiver end may create a terrific traffic in the network.

Attack 3.9.1 Acknowledgement spoofing.

3.10. Cloning

Attack 3.10.1 Cloning/Application Layer.

© 2016, IJCSMC All Rights Reserved

3.11. Impersonation

Attack 3.11.1 Node Replication. Also called Multiple Identity, Impersonation. An attacker seeks a node, tries to replicate the node, and impersonates as the node and tries to communicate with the other nodes as the original one.

3.12. Eavesdropping

Attack 3.12.1 Monitor and eavesdropping. Also called confidentiality. Attacker tries to listen the conversation and tries to find out the pattern of the communication such that the attacker can discover the confidential data.

3.13. Traffic Analysis

Attack 3.13.1 Traffic Analyses. Analysing the traffic that passes through the network and the attacker finds out the which node is being flooded with the messages, so that the attacker tries to extract the information from the flooded node.

3.14. Mote Class

Also called Insider Attacks. The attacker environment has authorized and unauthorized nodes. Authorized nodes help in supporting the unauthorized nodes in getting involved in the data transfer in the communicative network. Usually virus and Trojan programs are used in suffocating the data transfer nodes and increasing the bandwidth of the network traffic between the communicative nodes.

Attack 3.14.1 Mote-class/Control of Sensor Node. Malicious programs, access cryptographic keys.

Protocols which are affected by Attacks:

- Key Management.
- Reputation Assignment Scheme.
- Data Aggregation.
- Time Synchronization.
- Intrusion Detection Systems.

IV. COUNTER MEASURES

Some of the counter measures are as follows:

4.1. Outsider attacks and link layer security

The majority cases of outsider attacks are against sensor network routing protocols which can be prevented by a simple link layer encryption and the authentication is done using a globally shared key. The major classes of attacks are not countered by the link layer encryption and the authentication mechanisms which are peculiarly designed for wormhole attacks and HELLO flood attacks. Although duplicatory actions may be prevented from joining the network, but nothing prevents the attacker from using wormhole attacks.

Link layer security mechanisms are used globally - a shared key is completely ineffective in the presence of insider attacks. Insiders could attack the network by spoofing or by injecting malicious program routing information, creating sinkholes, selectively forwarding packets, also using the Sybil attack, and by broadcasting HELLO floods. The most sophisticated defense mechanisms are needed for providing reasonable protection against the wormholes and the insider attacks.

4.2. The Sybil attacks

An insider cannot be prevented from participating in the network, but the attacker can be an outsider. Verification of the insider should be strictly followed i.e., unauthorized access by the participant should be strictly prohibited. Now, by the prevention of the insider, the insider cannot

© 2016, IJCSMC All Rights Reserved

include or support the outsider who might be the attacker of the ensuing network.

4.3. HELLO flood attacks

The simplest defense against the HELLO flood attacks is to verify the bidirectionality of the link before taking a meaningful action based which is on a message that is received over that link. The identity verification protocol is much sufficient to prevent HELLO flood attacks..

4.4. Wormhole and Sinkhole attacks

Wormhole and sinkhole attacks are difficult to defend against, especially when the two nodes are under combination. Wormholes are hard to detect because they are private and out-of-band channel which are invisible in the underlying sensor network.
Sinkholes are another attacks which are difficult to defend against the protocols which are used in adverting the information such as remaining energy or providing an estimate of an end-to-end reliable communication for constructing a routing topology. A technique for detecting wormhole attacks is presented completely in [10], but this also requires an extremely very tight time and acknowledgement synchronization and is much infeasible for much wireless sensor networks. Because, these are extremely difficult to redesign the existing protocols with defensive mechanisms which are against these attacks, one such best solution is to carefully design a routing protocol which provides both the hole (wormholes and sinkholes) attacks meaningless.

4.5. Authenticated broadcast and flooding

When the base stations trustworthy, duplications of nodes will not be able to spoof, broadcast or flood messages from any of the base stations. This requirement needs some level of asymmetry: every node in the network can be potentially duplicated or compromised, no node would be able to spoof messages from the base stations, yet every node should be able to verify them. Authenticated broadcasting is useful for localized node interactions between node stations. Many protocols usually require nodes to broadcast HELLO messages to their neighbors. These messages should also be authenticated and is so impossible to spoof. So many proposals are proposed for authenticated broadcast which are intended for the use in a more conventional setting which involves either the use digital signatures and/or have packet overhead which well exceeds the length of typical sensor network packet. TESLA [12], a protocol proposed is very efficient, authenticated broadcasting technique and flooding which uses only symmetric key cryptography and also requires minimal packet overhead. SPIN [13] and other gossiping algorithms [14], [15] are the other techniques which are to reduce the messaging costs and collisions which are still achieve with robust probabilistic dissemination of messages send to every node in the wireless network.

4.6. Threats and countermeasures - OSI Layer wise

In this section, we are to discuss about some of the known threats and its countermeasures that are to be classified in the different OSI layers.

Physical Layer: In the below Table, we describe the Threats & Countermeasures of Wireless Sensor Network in the Physical Layer.

Table 1 Threats & Countermeasures of Wireless Sensor Network in the Physical Layer

Threat	**Countermeasure**
Interference	Channel hopping and Blacklisting
Jamming	Channel hopping and Blacklisting
Sybil	Physical Protection of devices
Tampering	Protection and Changing of key

Data-link Layer: In the below Table, we describe the Threats & Countermeasures of Wireless Sensor Network in the Data-Link Layer.

© 2016, IJCSMC All Rights Reserved

Table 2 Data-link Layer Threats and Countermeasures

Threat	Countermeasure
Collision	CRC and Time diversity
Exhaustion	Protection of Network ID and the other information that is required for joining the device
Spoofing	Using different paths for re-sending the message
Sybil	Regularly changing the key
De-synchronization	Using different neighbours for the time synchronization
Traffic analysis	Sending a dummy packet in the quite hours; and regular monitoring the WSN network
Eavesdropping	Key which protects DLPDU from the Eavesdropper

Network Layer: In the below Table, we describe the Threats & Countermeasures of Wireless Sensor Network in the Network Layer.

Table 3 Network Layer Threats and Countermeasures

Threat	Countermeasure
Wormhole	Physical monitoring of the Field devices and regular monitoring of the network which is done using Source Routing method. Monitoring system may use Packet Leach techniques
Selective forwarding	Regular network monitoring (using Source Routing)
DoS	Protection of the network specific data like Network ID etc. Physical protection and inspection of the network.
Sybil	Resetting of devices and changing of the session keys.
Traffic Analysis	Sending a dummy packet in quite hours; and regularly monitoring the WSN network.
Eavesdropping	Session keys protect NPDU from Eavesdroppers.

V. CONCLUSION

The security in Wireless Sensor Network plays an important role in the acceptance and use of sensor networks. In acuteness, a product of Wireless Sensor Network in the industry will not get its ensured acceptance until and unless there is a fool proof security to the network. In this paper, we have made all the possibilities of threat analysis which may occur to the Wireless Sensor Network and also have suggested some counter measures along with the further implementation to the advancement that is Smart Grid Technology. The Link layer encryption and authentication mechanisms are a reasonable approximation of defense which is against the remote class outsiders, it is to be considered and noted that cryptographical methods are not enough to defend the laptop-class adversaries and insiders: most careful and precautious protocol implementation is needed.

© 2016, IJCSMC All Rights Reserved

REFERENCES

[1] S. Sharma, "Energy-efficient Secure Routing in Wireless Sensor Networks", Dept of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela, Orissa, 769 008, India, 2009.

[2] D. Boyle, T. Newe,"Securing Wireless Sensor Networks: Security Architectures", Journal of Networks, 2008, 3 (1).

[3] X. Du, H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications,
2008.

[4] J. Granjal, R. Silva, J. Silva, "Security in Wireless Sensor Networks", CISUC UC, 2008.

[5] Y. Zou, K. Chakrabarty, "Sensor deployment and target localization based on virtual forces", INFOCOM 2003. Twenty- Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, Volume: 2, Pages: 1293 - 1303, April 2003.

[6] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley.

[7] J. R. Douceur, "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002.

[8] Castro and Liskov, "Practical byzantine fault tolerance," in OSDI: Symposium on Operating Systems Design and Implementation. USENIX Association, Co-sponsored by IEEE TCOS and ACM SIGOPS, 1999.

[9] A. Banerjea, "A taxonomy of dispersity routing schemes for fault tolerant real-time channels," in Proceedings of ECMAST, vol. 26, May 1996, pp.129-148.

[10] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

[11] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," Mobile Computing and Communications Review, vol. 4, no. 5, October 2001.

[12] A. Perrig, R. Szewczyk, V.Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," in Proceedings of Mobile Networking and Computing 2001, 2001.

[13] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, vol. 8, no. 2-3, pp. 169-185, 2002.

[14] M.-J. Lin, K. Marzullo, and S. Masini, "Gossip versus deterministic flooding: Low message overhead and high reliability for broadcasting on small networks, Tech. Rep. CS1999-0637, 18, 1999.

[15] L. Li, J. Halpern, and Z. Haas, "Gossip-based ad hoc routing," in IEEE Infocom 2002, 2002.

[16] Mona Sharifnejad, Mohsen Shari, Mansoureh Ghiasabadi and Sareh Beheshti, A Survey on Wireless Sensor Networks Security, SETIT 2007.

© 2016, IJCSMC All Rights Reserved