A STUDY OF SECURITY CHALLENGES IN WIRELESS SENSOR NETWORKS

KUTHADI VENU MADHAV[1] , RAJENDRA.C[2] AND RAJA LAKSHMI SELVARAJ[3]

[1] University of Johannesburg South Africa,
[2]Audisankaara College of Engineering and Technology, Gudur, Nellore , Andhra Pradesh, INDIA
[3] Botho College Gaborone, Botswana,

ABSTRACT

Wireless Sensor Networks (WSN) is a recent advanced technology of computer networks and electronics. The WSN increasingly becoming more practicable solution to many challenging applications. The sensor networks depend upon the sensed data, which may depend upon the application. One of the major applications of the sensor networks is in military. So security is the greatest concern to deploy sensor network such hostile unattended environments, monitoring real world applications. But the limitations and inherent constraints of the sensor nodes does not support the existing traditional security mechanisms in WSN. Now the present research is mainly concentrated on providing security mechanism in sensor networks. In this context, we analysis security aspects of the sensor networks like requirements, classifications, and type of attacks etc., in this survey paper.

Keywords: *Wireless Sensor Networks, Security, Survey*

1. INTRODUCTION

The sensor network is a group of self- organized, low priced sensor nodes and creates network in spontaneous manner. The WSN combines sensing, computation and communication in a single small device, called Sensor Node. The sensor node mainly contains radio, battery, microcontroller and power devices. Another term of sensor node is "mote". The sensors in a node provides the facility to get the data like pressure, temperature, light, motion, sound etc and capable of doing data processing. The main goal of the applications is achieved by the cooperation of all sensor nodes in the network. There are many sensor network applications like such environmental data collection, security monitoring, medical science, military, tracking etc. when sensor networks are randomly deployed in a hostile environment, security becomes extremely important factor. Because sensed data of sensor nodes is prone to different types of malicious before reaching base station. Security mechanisms are needed in communication part of the networks to provide safe data. The security is also important concern to get full advantageous of in-network data processing sensor networks. Protecting such a sensed data is complicated task.

Even through wireless sensor network is an advanced technology of network, it is extremely different from traditional wireless networks. This is, due to the unique characteristics of sensor nodes in WSN. So existing security mechanisms of traditional wireless networks are not directly applied in WSN. Sensor networks are closely interacting physical environment. So sensor nodes are also deployed in all areas even physical accessible attacks and broadcasting sensed data in network. So these reasons give a scope to new security mechanism rather than applying existing traditional security mechanisms in WSN.

Here, we outline unique properties of wireless sensor networks in section – II, challenges and requirements of security in sensor networks in section–III and existing security mechanism of WSN are discussed in section-IV. Finally section-V gives the conclusion and future work in wireless sensor network security area.

2. UNIQUE CHARACTERISTICS OF WSN

Presently, many of the motes are available in market with low prices. Some of them are Mica motes, Mica2 motes, Micaz motes, Intel motes, Berkeley motes, TelosB and Sunspot.

Table 1: Different Mote Characteristics

Types of motes	Mica	Intel	Sunspot
Processor	Atmel ATmegal128L (128 kb)	ARM7TDMI (12 MHz)	ARM920T (180MHz,32 bit)
Memory	4K RAM 512Data Flash 128Prog Flash	64 KB RAM 512 KB flash	512 K RAM 4M Flash
Radio	IEEE 802.15.4	30 mm range	IEEE 802.15.4
Size	58X32X7mm	29X29X9mm	
Data rate	250 kbps	250kbps	

By observing Table.1, and unlike, nodes in traditional wireless networks, nodes in wireless sensor networks have unique characteristics. These characteristics put more effort on security mechanism in sensor networks. The unique properties of sensor networks are, firstly sensor nodes are tiny devices and small in volume. Secondly sensor nodes have very limited storage capacity. It is the one of characteristic that does not support existing traditional wireless network's security mechanisms in WSN, because traditional security mechanisms require more storage capacity. Sensor Nodes are also need memory for operating system, in-network data processing and temporary data. So sensor nodes have inadequate memory for traditional security mechanism. Thirdly, sensor network has limited resources. So computational power in WSN is very less compared to traditional wireless networks. The existing traditional security mechanism has procedures like key establishment, encryption and decryption. These procedures need more computational power resources. .Fourthly, sensor nodes in WSN are battery based. So a node life time is directly depends on battery. Thus power consumption for any task should be decrease as much as possible.

The sensor nodes in WSN are connected in away that, they should participate and distribute the work for goal of applications. The nodes in sensor networks are connected in wireless manner and sensed data is broadcast in network. So the probability of collision and congestion is more. It gives more scope to trapping the sensed data in a network. Tree – routing uses in sensor networks to communicate data. In this, root node distributes work load to interested nodes in network. The inaccurate data effects the goal of the sensor applications. In-network data processing and filtering in WSN greatly saves the power efficiently. These sensor properties lead to a number of constraints and characteristics that have security implications.

3. SECURITY CHALLENGES OF WSN

3.1 Security Requirements in WSN:

The objective of confidentiality is required in sensors environment to protect information traveling among the sensor nodes of the network or between the sensors and the base station from disclosure. Authentication in sensor networks is essential for each sensor node and base station to have the ability to verify that the data received was really sent by a trusted sender or not. This authentication is needed during the clustering of sensor node in WSN. We can trust the data sent by the nodes in that group after clustering. Integrity controls must be implemented to ensure that information will not be altered in any unexpected way. Many sensor applications such as pollution and healthcare monitoring rely on the integrity of the information to function with accurate outcomes. Secure management is needed at base station, clustered nodes, and protocol layer in WSN. Because security issues like key distribution to sensor nodes in order to establish encryption and routing information need secure management.

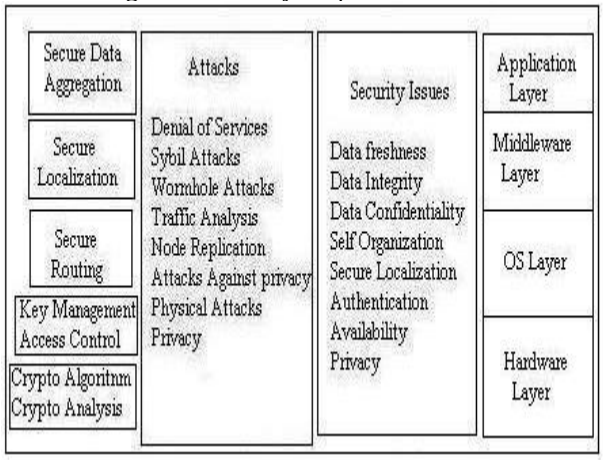
3.2 Attacks in WSN

The basic categories of attacks against privacy in sensor networks are eavesdropping, disruption and hijacking. The eavesdropping is used to know the output of sensor networks by listing transmitted messages of sensor nodes. There are mainly two ways to know about output data by concealing from sensor nodes or sending queries to sensor nodes or root nodes or aggregation points or attacks sensor nodes. The former approach is called passive eavesdropper and later approach is called active eavesdropper. The location of eavesdropper plays major role in getting information. This attack affects the property of confidentially, authentication in WSN. So proper encryption mechanism, message authentication code are needed before broadcasting data. The disruption mainly influences output of the network. The semantic disruption injects messages, corrupts data or changes values in order to render the aggregate data corrupted, useless and incomplete. Physical disruption renders the sensor readings by directly manipulating the environment. The hijacking approach is used to

take the control over sensor node in network. The hijacking mechanism gives more power to eavesdropping and disruption by hijacking main sensor nodes.

Another major attack in WSN is Denial of Service attacks. Some of the denial of service attack are at routing layer, link layer and transport layer. One of the denials of service attack is jamming networks. That is simply interfaces transmission frequency of WSN. There are mainly two types in jamming. In constant jamming, no messages are able to send or receive by a node in WSN. So this is complete jamming of network. In Intermittent jamming, the nodes are exchange messages with highly risks. Another new attack in WSN is Sybil attack. This Sybil attack is defined as a "malicious device illegitimately taking on multiple identities". This attack is affecting redundancy mechanism, routing algorithms, resource allocation procedure and data aggregation mechanism. With little effort, an adversary may capture nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locations within the network. They may allow the adversary to corrupt network data or even disconnect significant parts of the network. This attack can change entire network goal. This attack affects Integrity, confidentiality.

Figure 1: Security Map of Sensor Networks



The Figure-1 clearly specifies different security issues, attacks and corresponding security mechanism in specified areas.

4. SECURITY MECHANISMS

Now days, the researchers are attracted by security concepts of wireless sensor networks. Many researchers have proposed some security mechanisms in wireless sensor networks. In this section, we are dealing several security mechanisms.

"secFleck: Public key cryptography in wireless senor networks" approach is used to provide the message security services as confidentiality, Integrity and Authenticity in WSN at computationally fast and lower energy utilization. To design and implementation of public key system in WSN needs new version hardware and software in mote. This approach is named as secFleck. It uses Trusted module platform chip at hardware level and some software primitives. This approach uses RSA algorithm to implement asymmetric public key system. This approach has taken smaller RSA exponent (65537) and key size (2048) to provide security levels. This approach uses new operating system called Flack OS (FOS). FOS is a c-based cooperative multi- threaded operating system with public key cryptography primitives like encryption, decryption, singing, signature verification etc. Even this approach works fine for message security level, the learning new OS functions is length and complicated process. It also needs new hardware to provide message security level.

"LiSP: A Lightweight security protocol for wireless sensor networks", aims to provide authentication without retransmission of keys and also provides scalability in computing. It uses symmetric key system approach. It uses temporary keys and master keys. Temporary keys (TK) are used to encrypt and decrypt data packets. The master key (MK) is used to send temporary keys to single node. After network had been deployed, this protocol automatically selects one group of cluster heads as key server. The key server is used to distribute the temporal key, authenticate new nodes and detect nodes that have been compromised. When a key server transmits a packet for the first time it contains the length of the TK buffer, the key refresh rate, and the initial TK. The need for a Message Authentication Code is eliminated because the nodes are able to implicitly authenticate the TK by checking to see if the new TK matches the sequence of the other TK's in the TK buffer. LiSP provides a great deal of protection from compromised nodes and key servers. The keying system with implicit authentication allows the sensor to quickly detect whether or not the key that was sent from the key server is authentic or not. As long as the refresh rate is not very fast the sensors will not run out of battery power at a fast rate. LiSP is very scalable because the key server does most of the calculations and the key server can change depending on whether the key server has been

compromised or not. This protocol is used to reduce the retransmission of keys and provides implicit message authentication scheme to reduce the overhead. The keying mechanism depends upon application of wireless sensor networks.

TinySec: A link layer security architecture for wireless sensor networks" is a light weight and link layer security protocol. It provides security services as message Integrity, message authentication and access control at routing level and Reply protection in Adversary. It supports two different security options. They are Authenticated Encryption and Authentication only. In the Authenticated Encryption, the payload is encrypted first and then packet is encrypted using MAC. In Authentication only, the packet is directly encrypted with MAC without encrypting payload. This approach is used Cipher Blocked Chaining to encryption. TinySec is independent of cipher, key scheme, application. The TinySec packets are more in size then WSN packets, due to this; it needs more computing and processing power.

"SPINS: Security Protocol for Wireless Sensor Networks". This protocol is used to provide security services as freshness, Authentication, Confidentiality and Integrity. The two-way authentication, data confidentiality, freshness and integrity are provided with the help of SENP scheme and Authentication for Broadcast messages is provided with the help of µTELSA scheme. A block cipher RC5 algorithm was used by SNEP But it gives chances to eavesdropping to get plain and cipher text in way. Due to semantic security is low in SNEP implementation.

The Localized Encryption and Authentication Protocol security mechanism provides confidentiality and authentication mechanisms in sensor networks. This mechanism uses four different keys for each sensor node and controller to maintain master keys. They are individual key, pair-wise key, cluster key and group key. The individual key is unique for each node and used to provide secure communication between node and base station. This key is pre-loaded into each sensor node before deployment. A cluster key is a shared key and is shared by all neighbor nodes in the cluster. It is mainly used for securing broadcast messages in cluster groups because in-network computation is done at the cluster heads in WSN. The pair-wise shared key used to provide secure communication and authentication between immediate nodes or one hop nodes in WSN. This key is used before transmitting cluster key in cluster group. It is generated when the same key nodes are deployed in a single hop distance. The group is also a shared key. This key is shared by base station and set of nodes for broadcasting encrypted messages. This key used for hop-by-hop translation messages. The nodes are stationary in this approach. This approach needs more resource in-terms of computation power, memory to store keys and processing resources. But according to sensor network characteristics, this approach is inefficient and power consumable. This approach does not give good results on security damaged sensor applications. This approach should be applied prior to deployment of sensor network application.

In Random key pre-distribution schemes, a centralized key server generates a large key pool at offline. This generation of keys is done in key distribution phase. In key discovery phase, each sensor broadcasts their key identifiers or private shared keys. Then sensor nodes get the information about neighbor and network information after processing shared keys. The communication of data has to be done by shared key authentication. Too many sensor nodes are usually deployed for any sensor applications. Assigning unique keys to sensor node is a cumbersome problem. Even thorough, this mechanism used modified schemes like Purely Random Key Pre-distribution and Structured Key Pool Random Key Pre-distribution are inefficient to assigning keys to nodes in WSN. The attackers make use of advantage of decentralized pool key generation.

Public cryptography such as such as Diffie-Hellman key establishment at booting stage in base station, gives single point of failure of sensor network. So to provide efficient security mechanism, decryption should be done at cluster nodes and communicates the nodes or distributes messages in hierarchical manner. This scheme reduces number of keys in network, resource utilization and make utmost impossible to attacker to hijack.

"Fast Authenticated Key Establishment Protocols for Self-Organizing wireless Sensor Networks" has a goal to provide efficient authenticated key transferring mechanism. It uses elliptic Curve Cryptography (ECC) to provide encryption for sensor nodes. Cracking the private key is very difficult even the size of ECC keys length is less. Public keys are used to authenticate keys certificates. So during the process of authenticate keys certificates, this approach is usually finds public keys. These certificates are generated by sensor node and security manager. This work is accomplished by computation server if needed. The main drawback of using this key establishment

protocol is that sometimes a computation server may be needed for some of the computations. The amount of packets that are exchanged to authenticate a key seems like lengthy process to authenticate a key. It is difficult to figure out the strength of this protocol. Because this depends upon the keys and they contains random values.

The adversary attack leads to node replication attack with little effort. One approach to detect the replication node in wireless sensor networks is centralized scheme. In the Centralized scheme, all nodes in the network transfers a list of their neighbor's claimed locations to a central base station. Then base station can examine the lists for conflicting location claims. Even through this approach efficient, the nodes closest to the base station will receive the brunt of the routing load and will become attractive targets for the adversary. This protocol is also delays revocation, since the base station must wait for all of the reports to come in, analyze them for conflicts and then flood revocations throughout the network. Suppose adversary attacks at base station then centralized approach is inefficient and does not do well. At this case, this protocol gives single point of failure. The network life time is also decreases due to high traffic at base station surroundings. Even through this approach detects all replicated node in easy way, it requires more storage area in each node and also requires communication messages.

Another scheme to overcome the difficulties in centralized scheme is Location Detection scheme. In this scheme, instead of implementing node replication detection scheme at base station, it process at node's neighbor. It uses a voting mechanism; it collects neighbor's opinions on the legitimacy of the node. This approach is unable to detect the clones (i.e. nodes giving support to adversary) in disjoint neighborhood in network. It fails to detect subvert and clone if they are more than two hops away. Due to these drawbacks, this protocol became inefficient to find replication nodes in WSN.

One simple approach to detect the distributed replication nodes is Simple Broadcast Protocol. In this approach, each node broadcast authenticated messages about their location and also stores the information about neighbor nodes. Even through this approach gives 100% results, it may not works if adversary attacks at key areas or communication paths. This approach costs more in form of communication for large networks.

One of the improvements of Simple Broadcast Scheme is Deterministic Multicast Protocol. The main of this approach is to reduce the communication of simple broadcast scheme by sharing the node's location to a subset of deterministically chosen node, called witness node. This subset may be fixed for a particular node. The witness nodes are selected based on function of node ID's and probability. So it uses multicast approach to give judgment over nodes location claim. Due to this, the number of message transfers in the network is decreased. This is also fails if adversary attacks or jams the messages in the network. Because it shares the node's location to a limited subset of deterministically chosen nodes only. This approach is not doing well, if any one of the witness node is caught by adversary.

"Distributed Detection of node replication attacks in wireless sensor networks", this paper deals with detection of node replication attacks due to adversary at protocol level (routing layer). It uses two routing algorithms such as Randomized Multicast and Line selected Multicast. This paper evaluated security at protocol level by using probability theory. The adversaries have to be detected as soon as it occurs otherwise replicated nodes are increases in next data gathering cycle. Assume that the adversary cannot readily create new IDs for nodes. In the cloned formation, this paper assumed to be at least one node as legitimate neighbor to clone. It also assumes the adversary in stealthy manner. Due to this, the detection of adversary is complex. So it uses one protocol that sweeps the network, using SWATT technique to remove compromised node and human interactions. Here it assumes that the adversary can read and write the messages using only nodes under adversary control. [i.e. read and writing messages should do in adversary control parts by adversary.] This is paper also works in a situation that, the adversary can change the topology of the network by adding replicas.

5. CONCLUSION AND FEATURE WORK

Security in wireless sensor networks has attracted many researchers, due to its unique characteristics, low cost deployment, and real environment orientation. This paper is mainly concentrated on key distribution mechanisms, detection of node replications and secure routing mechanisms in WSN. The existing security mechanisms are providing security to some extent only. Several constraints and deployment environment of wireless sensor networks makes the security is cumbersome task than traditional wireless network security mechanisms. In order to achieve full security in WSN, implementation of

security mechanism would be done on each component of sensor networks. The future work should consider the characteristics of sensor network and communication protocols. This mechanism should provide less power consumption in wireless sensor networks.

REFERENCES:

[1] M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, "Sensor Network Security: More Interesting Than You Think", In Proc. of the 1st USENIX HotSec, 2006.

[2] M. Anand, Z. Ives, and I. Lee. "Quantifying Eavesdropping Vulnerability in Sensor Networks", In Proc. of the 2nd International VLDB Workshop on Data Mgnt. for Sensor Networks (DMSN), 2005.

[3] G. Gaubatz, J.-P. Kaps, and B. Sunar. "Public key cryptography in sensor networks", – Revisited. In Proc. of the 1st ESAS, 2004.

[4] A. Perrig, J. Stankovic, and D. Wagner. "Security in Wireless Sensor Networks", Communications, ACM, 47(6):53–57, 2004.

[5]http://www.cs.wayne.edu/weisong/papers/walters05-wsn-security-survey.pdf

[6] Adrian Perrig, John Stankovic, and David Wagner, "Security in wireless sensor networks", Communications of the ACM. Vol 47 (6), pp. 53-57, 2004. Xiuli Ren and Haibin Yu, "Security Mechanisms for Wireless Sensor Networks", International Journal of Computer Science and Network Security, Vol. 6, No.3, March 2006.

[8] Frederik Armknecht, Alban Hessler, Joao Girao, Amardeo Sarma and Dirk Westhoff, "Security solutions for wireless sensor networks", WWRF 17, 2005.

[9] Malan D. J., Welsh M., and Smith M. D.," A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography" In First IEEE International Conference on Sensor and Ad Hoc Communications and Networks SECON04, 2004.

[10] Wen Hu, Peter Corke, Wen Chan, et al., "secFleck: A Public Key Technology Platform for Wireless Sensor Networks.", EWSN, volume 5432 of Lecture Notes in Computer Science, page 296-311. Springer, (2009).

[11] C. Karlof, N. Sastry, and D. Wagner. "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", SenSys '04. Pages 162-175. November 3-5.

[12] T. Park and K. Shin. "LiSP: A Lightweight Security Protocol for Wireless Sensor Networks". ACM Transactions on Embedded Computing Systems, Vol 3, No. 3, Pages 634-660, August 2004.

[13] A. Perrig et. al. "SPINS: Security Protocols for Sensor Networks. Wireless Networks", vol. 8, 2002, Pages 521-534.

[14] Q. Huang et al. "Fast Authenticated Key Establishment Protocols for Self- Organizing Sensor Networks", WSNA '03, September 19, 2003, Pages 141-150.

[15] Parno .B, Perrig .A, Gligor .V, "Distributed Detection of Node Replication Attacks in Sensor Networks", IEEE Symposium on Security and Privacy, 2005.