ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Security Attacks and Its Countermeasures in Wireless Sensor Networks - A Survey.

B Kiruthika*, SAbinaya, R Ezhilarasie, and A Umamakeswari.

School of Computing, SASTRA University, Tirumalaisamudram, Thanjavur-613401, Tamil Nadu, India.

ABSTRACT

Advancements in hardware manufacturing and the enhancements of effective software mechanisms has led to development of networks consisting of cost-effective sensor nodes communicating via wireless medium. These networks are termed as Wireless Sensor Networks (WSN). Although many communication protocols are designed for routing, security is a threat to these networks. In this paper, we present an overview of wireless networks, how they differ from other networks and the underlying security issues are discussed. The conventional attacks on WSN are summarised and survey presents several security issues related to it.

Keywords: WSN, Security, Attacks, Sensor nodes, Security issues.

Corresponding author

ISSN: 0975-8585

INTRODUCTION

The major issue in switching from wired to wireless networks is security. However, there are more efficient security solutions for wired network and cannot be implemented to wireless networks. Achieving security in MANETs is more complex than wired networks and Internet. It is much more complex to provide security schemes in WSN as these networks are limited in resources.

WIRED VS WIRELESS NETWORKS

Wireless networks are more flexible to both end users and network operators. It provides abundant network coverage over a wide area at minimum cost as it eliminates cost required for wires. This is useful for several applications where implementation of wired networks in difficult. WSN provides support for mobile sensor nodes.

The security threats in wireless networks include that of wired. Moreover, wireless networks possess additional threats due to unreliability in wireless channel, access control, power mechanisms, complexity in system design, routing mechanisms.

MANETs Vs WSN

WSN are widely used in many applications due to its ad-hoc nature. Though several protocols have been designed for wireless networks, they are not applicable to all applications. The basic differences between an ad hoc network and WSN are as below:

- Number of nodes deployed in sensor network is greater than the nodes in ad hoc networks.
- Deployment of nodes is dense.
- Nodes are subject to failures due to resource limitations imposed on it.
- Network topology changes based on the requirements.
- Ad hoc networks uses point-to-point mechanisms, whereas sensor networks uses broadcast mechanism.
- Each node in sensor network does not have any identification number assigned to it as it may add overhead to the network.

ORGANISATION OF THE PAPER

Although various challenges are implied in WSN, this paper focuses on various security issues and measures to overcome those. Designing a security scheme for WSN is challenging due to the resource constrained nature of the network. Section 2 presents an overview of WSN and its requirements. Section 3 presents about the security requirements in WSN. The taxonomy of several attacks applicable to WSN is described in Section 4. Section 5 emphasises on issues in security mechanisms.

WIRELESS SENSOR NETWORK

OVERVIEW OF WSN

Wireless sensor networks are large network containing tiny sensor nodes that communicates through a wireless medium. These sensor nodes are resource constrained devices that has predefined functions to accomplish the objectives of intended applications. The main components of WSN are the sink nodes and the sensor nodes that forms the network [1]. Sensor nodes are autonomous, capable of forming a network in the deployed environment. These nodes can be either deployed at locations determined by a deterministic scheme or at random locations. Depending on the application requirements, these nodes are either static or mobile. A sink node, often termed as base station [2] (BS) is deployed to control the network.

After the deployment, the sensor nodes continuously monitor the environment. On occurrence of an event, a nearby sensor node detects it. It collects and transmits information about the event to every other node in the network via BS. Upon receiving it, the BS can process and forward it to the external authority. This authority can command or request query to BS, which in turn broadcasts these messages to other nodes in the

ISSN: 0975-8585

network. Thus, a Base Station can act as gateway between the network and other peripherals. An example of WSN is demonstrated in Figure 1.

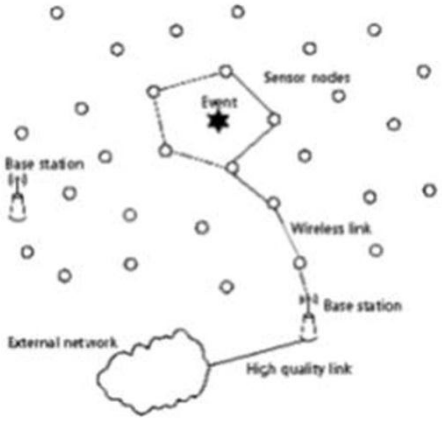

Figure 1: Wireless sensor network

HARDWARE FEATURES

Based on the requirements of the application, the hardware components have to be chosen for the network. The sensor node is an integration of both hardware and software. It senses, processes and communicates the data acquired from the environment. It requires a wireless medium for transmitting and receiving the sensed data over the network [3]. The basic components present in a sensor node are described in Figure 2.

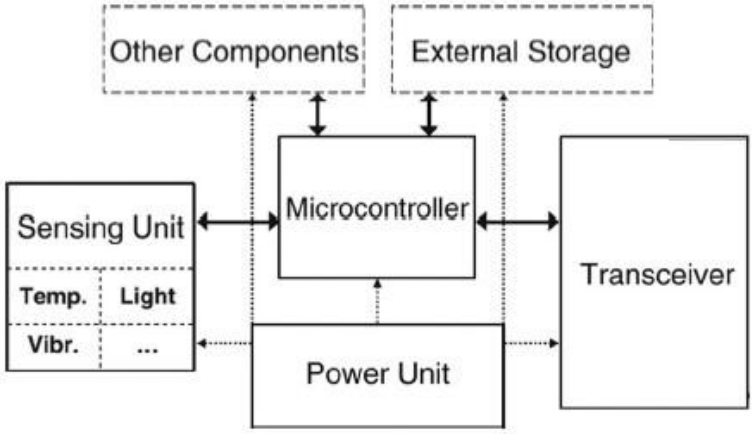

Figure 2: Sensor node Architecture

A sensor node consists of various functional units: Sensor unit, Processor unit, Transmission unit and Power unit. Depending on the application requirements, various other functional units can be added to the node. The sensing unit observes and gathers information about the deployed environment. The data obtained is transferred into digital by ADC and is forwarded into processor unit. Processor unit comprises of a memory unit, controls the processes handled by other nodes in the network to achieve the objective of the application. Transmission unit establishes communication in network. The sensor nodes are battery powered devices; hence it essential to adopt methods for extending the life time of the nodes.

Software Features

OPERATING SYSTEM (OS)

As WSN are resource constrained, traditional operating systems are not applicable. A new form of OS has to be designed with the following features [4]:

- Act as platform between the users to middleware/ application software.
- Provide Real- time support and resource management schemes.
- Consume less power and incorporate power management schemes.
- Memory required should be less.
- Provide parallel processing with threads for multi sensor operations.

QUERYING POLICIES

In order to provide efficient deployment, maintenance and handling of sensor information, a storage medium and query mechanisms is mandatory. The storage medium is often a database. It is capable of storing dynamic information [5]. For sophisticated queries, a web based system is provided. Query mechanisms poses various challenges as the sensor nodes are resource constrained and they involve continuous sensor data.

Protocol Stack

The sensor node protocol stack [6] is illustrated in Figure 3. It combines all the units of the sensor node. The physical layer handles the modulation and communication schemes. The modulation schemes involves choice of frequency, generation of carrier frequency, processing and detection of various signals. Data Encryption is also performed at this layer. The access and flow controls of the data frames in the communication network is managed by data link layer. Routing of data from the transport layer is accomplished by the network layer. The data flow can be effectively managed by the transport layer and provides accessibility to WSN via Internet or other systems.

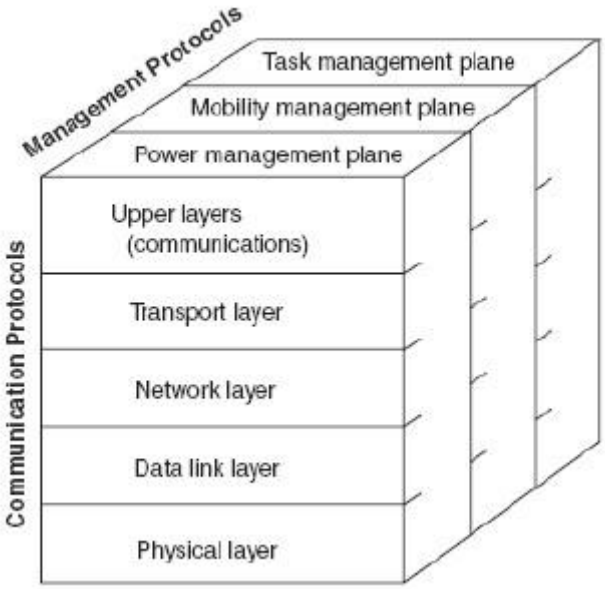

Figure 3: Generic Protocol stack

Depending on the application requirements, various application software can be used. Power saving schemes can be incorporated to save energy consumption. Mobile nodes are tracked and managed to synchronise with other nodes in the network. Scheduling mechanisms are applied for managing tasks in a sensor node.

RESOURCE CONSTRAINTS ON SENSOR NODE

A sensor node consists of processor of frequency range 4-8 MHz; Memory- 4KB RAM; Flash memory - 128KB and Radio frequency -916 MHz, Various constrains imposed on WSN are as follows:

Autonomous Large number of nodes are deployed in random manner in hostile environments where the human intervene is less. In such conditions, the nodes must be capable of establishing network with other nodes to form the network.

Bandwidth In order to reduce the energy consumption, communication range of the nodes are limited.

Energy consumption WSN nodes are battery powered and have less form factor. Protocol implemented on the network must consume few messages. Hardware components performing other functions consumes considerable amount of energy. Of all the units in a node, energy consumed by the communication unit is high. Additional mechanisms for cryptographic operations consumes more energy.

Memory Requirements Sensor nodes can store only limited amount of data. The amount of data stored by the protocol has to be less.

Scalability The number of nodes required to form the network must be in the range of few hundreds to thousands to provide effective coverage.

Tolerance Due to various reasons in the deployed environment, the nodes may fail to perform the task assigned to it. Fault tolerance mechanisms has to be adopted to improve the network utility.

PERFORMANCE MEASURES

The following parameters are used to evaluate the performance of WSN [7,8]:

Accuracy Attaining a high accurate data can be achieved by collaborating various sensor node data in the network.

Communication Range Multi- hop communication links can be used to encompass coverage over large area. Although this method advantageous this may result in high energy consumption and it reduces the network's lifetime.

Computation Managing the communication protocols and providing in-network data processing are the computational operation performed at the network. High communication standards requires faster computing capabilities.

Cost-effectiveness The cost required for maintenance of the nodes has to be less than the cost required for initial deployment.

Latency/Throughput Based on the application requirements, the data has to be transmitted with/without delay in the network. The facility to have less difference in response time tends to increase lifetime.

Lifetime As the sensor nodes are battery operated, efficient methods has to be incorporated to prolong the network lifetime.

Robustness Sensor nodes must be able to account for link failures. In-network communication among the nodes must be established to provide effective data processing.

Security Sensor data transmitted in the network has to be secured by using cryptographic authentication methods. The data stored at individual nodes are also to be secured.

APPLICATIONS

The services provided by WSN are: monitoring, providing data when required and alerting. Based on the above mentioned services, WSN is used various applications:

Environmental applications: These applications induces tracking the movements of flocks, monitoring climatic conditions and providing solutions for irrigation.

Home applications: One of the key applications of WSN is home automation that allows the end user to control devices at home.

Medical applications: Provides an interface for the elderly people, monitoring systems for patient, diagnostics, maintaining the patients' health information.

Military applications: WSN are used for surveillance and control applications. They can be essential part of commanding, controlling, communicating, computing, intelligence, surveillance, reconnaissance and targeting (C4ISRT) schemes.

Other commercial applications: Other area in which WSN is widely used are: disaster management, vehicle tracking, robot control, plant control and automation.

SECURITY

NEED FOR SECURITY

Sensor networks are established in hostile locations which involves sensitive data transmission within the network. In such applications, security of the data is critical. However, securing this information is more complex due to the limitation in resources of the networks. The sensor networks monitors and deduce information about the surroundings(9). This may result in leakage of information and facilitates for other threats. These issues demands security during the design time of the network to assure safe operation, privacy of sensor data.

COMPLICATIONS IN WSN SECURITY

The following are the complications implied on WSN [2,9]:

- The cost of the network has to be maintained minimum.
- The nodes are often prone to failure due to cost effective network.
- Malicious data can be injected easily into the network through the wireless medium.
- Anti-Jamming methods consumes high energy and requires complex circuit designs.
- Attacks such as Denial-of-Service (DoS), eavesdropping, information leakage can be a threat due to the ad-hoc nature of WSN.
- Providing security to large number of nodes becomes complex.
- Compromise has to be made on minimal resource usage and maximum security.
- Choice of has to made on efficient and suitable crypto techniques.

SECURITY SERVICES

The aim of security is to offer services to protect against various threats [10]. Various analysis has been made on vulnerability in design principles. The security services offered are [11]:

- *Access-control* manages and averts unauthorised access in the network.
- *Anonymity* hides information about the originator of data.
- *Authentication* assures that the receiver or sender of the packet is an authorised node.
- *Authorization* approves neighbour node's information either to be received or updated. *Availability* is the capability to sustain network operations without any intermission due to threats.
- *Confidentiality* is required to avoid an attacker from carrying out traffic analysis.
- *Degradation of services* is the ability to adapt security mechanisms based on the available resources.
- *Freshness* prevents resending of previously received packets from a faulty node. *Forward/Backward secrecy* node must not be capable of retrieving future/previous data after it is transmitted.
- *Integrity* ensures unmodified packet transmission in the network.
- *Non-repudiation* authenticates the packet's source i.e. checks the source and ensures that it has sent the packet.
- *Privacy* secures sensitive data from an attacker obtaining information.

- *Resilience* capability of the sensor network to operate in case of node compromises.
- *Survivability* ability to deliver a least service in cases of failures, energy loss or attacks.

PRINCIPLES FOR SECURING WSN

Various principles have been proposed for addressing the security problems in WSN. Dynamic configuration of different security services can be one of solutions. However, the security of a sensor network is ensured at all layers. In case of large node deployments, the nodes has to be cooperative for dynamic reconfiguration and shall be managed by a decentralised node. The cost of providing security must not exceed cost incurred due to threats [12]. Traditional security approaches may not be applicable to WSN due to the limitations imposed on the sensor nodes. A *holistic method* [13] ensures security over all layers in the network. A security solution for each layers may not suffice for such network and is must ensure solution for all layers in the protocol stack. Although layered schemes are advantageous it has certain limitations:

- Designing individual protocols for different layers may be redundant but the resource required is high.
- A counterattack mechanism to encounter attacks in various layers may not assure security.
- Power consumed by any security mechanism cannot be addressed by each layer in the stack.

To overcome the above, *a cross-layer method* [14] can be implemented to reduce the resource utilisation.

TAXONOMY OF ATTACKS

WSN is prone to various threats because the communication among the nodes is achieved by a wireless medium. Moreover, the nodes are tend to operate in environments where the nodes may suffer physical attacks. It becomes impractical to manage large scale nodes in such environments where human intervene is difficult. Different types of attacks may be imposed on the system. This section briefly describes the classification of WSN security based on various layers in the network and ability of the intruder. Various defence mechanisms proposed in the literature are also presented.

BASED ON ABILITY OF INTRUDER

INSIDER VS OUTSIDER ATTACKS

Insider attacks are caused when appropriate sensor nodes perform in inadvertent or unauthorized manner; outsider attacks are described as attacks imposed by nodes that are anonymous to the network. Robustness towards Outsider Attacks [9] and Resilience towards Insider Attacks has to be possessed by the nodes. In addition to it, nodes may also serve for node compromises and provide various levels of security to the data.

ACTIVE VS PASSIVE ATTACKS

Active attacks are ones that involves altering the original data stream or creating a false data stream; Passive attacks involve observing or eavesdropping data exchanged in the network.

LAPTOP CLASS VS MOTE CLASS ATTACKS

Laptop class attacks involve effective strategies to attack the network. It involves devices with high range for transmission, computation capability and power saving ability than the sensor nodes; Mote-class attacks are made with nodes having similar potential to the nodes in the network.

ATTACKS ON DATA IN TRANSIT

In WSN, the nodes observe the variation of particular parameter and notify it to the base station. During the transmission of report, the data in transmit might be attacked to feed erroneous data to the sinks(15).

FABRICATION

The attacker introduces incorrect information and negotiates the reliability of data. It intimidates accuracy of the information. The key idea is to obscure or deceive the nodes participating in the communication. This action may result in information flooding in network and DoS attacks.

INTERCEPTION

The network becomes compromised when the attacker obtains an access to the nodes or information in it. Node capturing is an example for this type of attack. This weakens the confidentiality of the information by eavesdropping the data exchanges and is to attack the application layer.

INTERRUPTION

The communication linkage in the network is lost. This threatens the service accessibility. The main intention is to initiate denial-of-service attacks and is aimed on all layers.

MODIFICATION

The unauthorized person gains access to the data and also alters it. This deceives integrity of data. This is made to mislead the nodes involved in the network and is intended at network layer as well as the application layer.

RESTATING EXISTING INFORMATION

This function focuses on newly obtained sensor information. The primary aim of this attack is to deceive the unsynchronised nodes.

BASED ON HOST AND NETWORK

ATTACKS ON HOST NODE

This type of attacks [16] can be made in three ways: *User compromise* this includes compromising of the network by obtaining the private information about the nodes. *Hardware compromise* includes damaging the hardware to obtain the information, crypto keys and program code stored in a node. The intruder may try to download erroneous program into it. *Software compromise* includes rupturing the software operating on the sensor nodes. The OS or the applications in the nodes are exposed to malfunctions such as overflow in buffer.

ATTACKS ON THE NETWORK

Network compromises can be introduced based on layers of the network or based on the protocol involved. These encompass all the data in transit attacks. It also involves Protocol deviation [16]: The main aim of the attacker is to obtain unauthorized advantage for utilising the network so as to alter the purpose of the network.

ATTACKS ON PROTOCOL STACK

The following segment examines the attacks on the various layers in WSN [17].

PHYSICAL LAYER

a) *Destruction/Tamper Proofing* An attacker, upon acquiring access to a sensor node, retrieves sensitive data. One of the approach is to design a fault tolerant protocol that makes the nodes capable of withstanding such attacks. Tamper-proofing(3)of a node is another defense mechanism in which the node deletes its contents by itself when a third party gains access to it. Another approach is by designing protocols for Fault Tolerant

b) *Jamming* An attacker tries to upset the function of the network by transmitting a high power radio signal to nodes involved in the network. This results in DoS [18] attacks and node compromises. This attack can be originated as: distortion of the packets transmitted in the network, transmission a deceived data stream that appears to be authentic, random switch between sleep state and jamming to reduce power consumption and transmitting jam signal on a network traffic. Spread-Spectrum techniques can be used to defend these attacks. Admission Control Procedure is required for handling jamming in the MAC layer. Network layer handles it by including both the routing and the jammed areas. Techniques combining received signal strength indicator (RSSI) values, packet delivery ratio (PDR) and average time necessary to sense an idle channel can identify all sorts of jamming.

c) *Radio interference*(19) the attacker introduces enormous interference either constantly or occasionally. Symmetric key crypto algorithms which discloses keys at delayed intervals can be used to overcome the issue.

DATA LINK LAYER

a) *Collision* When any two nodes involved in the network attempts to send data on same frequency instantaneously, a Collison [19] occurs. It alters the data portion of the packet, causing a mismatch in the checksum at the receiver end and the packet is discarded. Error-coding techniques can be used to avoid collisions.

b) *Continuous Channel Access* Media Access control protocol can be disrupted by a malicious sensor node by acquiring the channel over a long period. This causes other nodes to starve for the gaining access over the channel. Rate Limiting, avoids unnecessary requests to channel prevents power depletion due to continuous transmission. Time-Division Multiplexing methods can also be used to assign time slots to the nodes for transmission.

c) *Interrogation* To overcome hidden-node problem, a two way handshake mechanism is used which includes request-to-send (RTS) and clear-to-send (CTS) to access the channel. The attacker can exploit the resource of the nodes by continuously transmitting RTS to prompt CTS replies from a directed node. To defense such attacks, a nodes can limit the number of connections it makes in the network or use an authentication mechanism.

d) *Sybil Attack* This attack is made on two ways: One in which a single node acts as number of Sybil Nodes and reinforces the data aggregation to be false. The other type involves Voting. MAC protocols uses voting for identifying a link for communication among the available ones. The Sybil Attack introduces a ballot box and thus the intruder obtains the results of voting. This type of attack results in partial DoS and degradation in performance of the network. Using small frames, such that a single node holds the channel for a lesser time duration can defense form such attacks.

e) *Unfairness* [18] A collision based MAC layer attacks or priority mechanisms may lead to unfairness in network.

NETWORK LAYER

a) *Acknowledgment Spoofing* Routing algorithms implemented requires acknowledgements. A malicious node can spoof these acknowledgements to a target node to provide false data. Authenticating the nodes thru encryption of packet header and transmitted information.

b) *Black Hole Attack* Assuming that nodes in the network are authenticated, the WSN uses a multi-hop links to transmit messages. However, the malicious nodes denies to route messages and discards them. A random selection of routes that does not overlaps with other links to destination can be used along with the multi path routing.

c) *Hello Messages* This attack uses Hello messages which is used by several protocols to broadcast information about the neighbouring nodes. Node upon receiving such messages might pretends to be present in coverage range of the transmitter. Laptop-class attack may broadcast such packet to every other nodes. It makes a compromised node to believe that it is still present in the network. This results in transmission of messages to an imaginary node. Authentication of neighbouring nodes is a solution to this problems. It can be avoided by bi-directional verification of communication link before performing actions the received message.

d) *Homing* performs traffic analysis to find and target nodes with high tasks i.e. nodes acting as cluster head or nodes managing the keys. By using jamming signals the attacker may establish DoS into the network. Encryption of the packet header is used a preventive measure. It involves introducing a dummy packet to

equalise the volume of traffic and block the traffic analysis. But this preventive measure may result in high energy consumption.

e) *Information altering, spoofing or replaying* a direct attack that can be induced in the routing protocol of the sensor network is to focus on the routing data that is exchanged among various nodes. The intruder might alter, replay or spoof the data to introduce traffic. Routing loops, introducing traffic into network originating from a selected node, altering the routes to source nodes, generating false messages, increasing the latency and splitting of the network. A message authentication code can be appended to the message to encounter such attacks.

f) *Internet Smurf Attack* floods the target node's link into the network. An attacker obtains a node's identity and broadcasts unwanted messages in the network. It also deceives responses to that node sent by other neighbouring node. In such situations, the node can enter into sleep mode thereby avoiding network flooding.

g) *Misdirection* A malicious node can mislead the packets by presenting a false routing path so that the destination node becomes unreachable. This may lead in other neighbouring nodes becoming a victim and results in flooding of unwanted message in the network. To overcome this the node may enter into sleep node.

h) *Node Capture* A single node captured by an attacker may be sufficient to take over the network.

i) *Sinkhole* [13] Based on routing mechanism, a sinkhole attack introduces traffic to a compromised node. Few protocols such as Geo-routing are resistant to these attacks as the topology of the network uses only localised data and traffic id routed to physical location of the base station. This makes it complex for an attacker to construct a sinkhole.

j) *Sybil Attack* Multiple identities are created for a single node to deceive other nodes. This might result in misleading the nodes and hence the link is trusted respective to that node. A symmetric key is assumed for each node and is stored at the sink node.

k) *Wormhole Attacks* An attacker might tunnel the data received over the channel in a part of the network and broadcast them into another part. Two malicious nodes working in coordination are used. The nodes are used to estimate the distance between each other by transmitting packets. Time synchronisation can be established among the nodes to overcome this attack. However, it is practically infeasible to implement in hostile environments.

TRANSPORT LAYER

a) *De-synchronization Attacks* [3] The attacker frequently fakes data to several end points and the node requests for the missed frames. The messages are retransmitted and if the attacker keeps a time, it may block the nodes from exchanging the original data. It results in depletion of energy in the node. An authentication schemes for all packets that accounts also for control fields in the frame is required. Authentication only for the header or for the whole packet is preferred.

b) *Flooding* Request for new connection is made repeatedly until the maximum limit is reached or resource of the nodes are depleted. A defense mechanism may be provided by requesting the nodes to solve its objective.

APPLICATION LAYER

a) *Reprogram attack* the network allows to remotely reprogram the deployed nodes in the network. If this process isn't secure, an attacker can obtain control of the network. Authentication mechanisms to protect this process.

b) *Overwhelm attack* the attacker may attempt to control the sensors and induce traffic into sink nodes. This attack drains the energy of the node and intakes large bandwidth. Efficient algorithms to perform aggregation of data and rate limiting can be used to reduce the effects of these attacks.

c) *Path-based DOS attack* Retransmission of packets into leaf nodes of the network may result in network traffic. Thereby, preventing other nodes from accessing the network. Authentication of combined packets can prevent such attacks.

ISSUES WITH SECURITY MECHANISMS

CODE ATTESTATION

As the sensor nodes are cost-effective and are prone to physical attacks. An attacker may try to compromise the node by altering the program. To avoid reprogramming of the nodes of the network by an unauthorized party, it is necessary for attesting the program codes before downloading it into the hardware. Further the damages can be reduced by periodical verification of nodes. Code attestation can be implemented both in hardware and software [20].

CRYPTOGRAPHY METHODS

It is important that the performance of cryptographic operations is high to achieve high security in WSN. The cryptographic operations such as authentication, encryption and so on. Appropriate methods has to be chosen to provide high level security in the network. The choice of crypto operation depends on the capability of the system components. As the sensor nodes are resource constrained, asymmetric cryptographic methods are expensive. Symmetric key algorithm are more efficient than public key algorithms. The encryption methods requires additional memory for transmission and computation. It also introduces a delay in the network. The following parameters are to be considered for selecting the appropriate algorithm [20]:

- The energy required to perform the cryptographic operations.
- Memory required to store the program, keys and the flash memory to store the temporary variables generated.
- The time needed to perform the functions.
- Protocols with high reliability and scalability has to be designed.

The security of the system depends on protecting the key. The computed key is exchanged among the nodes for initiating the communication. Key management methods are used to determine and exchange various keys in the networks. The types of keys include: Pair-wise keys, Group keys and individual keys. The entire system becomes open when an attacker is able to interpret the key. An end-to-end encryption of messages may not be applicable for large number of nodes as the nodes are insufficient to store the keys. Various hoping methods can used for encryption so that the sensor nodes can share its key with its neighbours. The issues related to key management design are:

- Public key algorithms costs less than the private key algorithms. A study can be made on efficient way for implementing private key methods.
- Although symmetric methods are better than public key methods, no appropriate method for distribution of keys.
- Symmetric key methods focuses on the link layer for a single hop communication network, and does not provide methods for multi-hop transport layer.
- For nodes that are connected by a multiple hop links needs a path-key assurance and secured end-to-end communication.
- Cryptography techniques based on identity can be used to provide authentication to public keys.
- It is complex to create a single key for key revocation schemes.
- Security of the sink nodes has to be verified by the key management methods.
- Designing of public key based key management schemes has to be designed for large scale nodes.
- Although key management methods accounts for security and node compromise, the performance is not high in various applications.
- Dynamic key management methods can be established for mobile nodes.

Key discovery method has to be designed such that the intruder cannot obtain key during exchange.

DATA AGGREGATION

As the WSN has various resource limitations, decreasing the communication of sensors and sink nodes is energy efficient. Data fusion [19] is a process intermediate nodes are involved. These nodes gathers the raw sensor information from the nodes and process it before forwarding it to other node. Such nodes are

termed as “aggregators”. This operation decreases the number of messages transmitted in the network. Due to nature of the environment, there is a possibility for compromise of aggregators. An attacker can introduce fake messages into the network. The issues involved in attacks this technique are given below:

- Mechanisms need to assure the accuracy of data from the aggregators and part of nodes in the network.
- The comparison has to be made on various available existing aggregation protocols based on several parameters.
- Cost-effective cryptographic methods for in-network processing can be developed. These must also offer authentication to aggregators.
- Aggregation methods considering the power consumption and mobile nodes may be designed.
- An aggregator in a network is assumed to possess high performance capabilities. Schemes may be developed in applications that do not have such nodes.

GROUP MANAGEMENT

The network is divided into several sub parts/groups [19]. The data received from a sensor is processed locally. An analysis is made on the data obtained as a result of aggregation at the cluster heads. The cluster head has the right to authenticate the information received from neighbouring nodes in a group. A group key management scheme can be used to maintain the keys. Adding a node or removing it from a group may create problem in the cluster heads. Subsequently, group management has to be secured.

INTRUSION DETECTION

One of the major unsolved problems in WSN is intrusion detection. Analysis made on the important parts of the network may not be sufficient. A centralised mechanism has to be designed to overcome this issue. The key areas to be focused are: resource limitations, packet injections, scalability of protocols.

LOCALIZATION OF NODES

The nodes are randomly arranged in an environment to perform assigned tasks. For effective operation of the network, the location of the sensor nodes must be identified in prior. This sensor information may also provide the location of the sensors to its neighbouring nodes. Various routing protocols are used to obtain the location information of the node. Methods based on estimation of angle/distance, position estimation and localization algorithms [21] are widely used.

LOCATION DISCOVERY

Location of sensor nodes [13] plays a vital role in many applications. It becomes easier for an attacker to estimate the location of the node and mislead the normal functions performed at the node. An attacker might offer incorrect location by beacon messages captured at various locations. A beacon node may be compromised and provide false location information. In many cases the non-beacon nodes manipulates the locations inaccurately. Approaches for location estimation are voting based method, minimum mean square estimation (MMSE) and an iterative mechanism to tolerate for false node locations.

ROUTING MECHANISMS

WSN nodes are often linked by a multiple-hop routing to exchange data among the nodes of the network. This may cause many attacks into the network. Various routing mechanisms [22] employing security mechanisms based on different attributes are designed. The attributes includes verification of node’s identity, confirmation of nodes on both directions, restrictions on structure of topology, decentralisation of the sink node and multiple path routing. Here are few methods to make security in routing mechanisms simple [23]:

- Node compromise mechanism with high parameter assumptions can be designed.
- Routing mechanisms may be developed for mobile WSN and are much complex than static networks.
- As the topology change occurs due to aging of the network, there are chances for erroneous messages being sent. Mechanisms for preventing such access can be provided

- Routing algorithms for hierarchical networks that includes cluster heads and end nodes can be defined.
- The quality of data in the network can be evaluated on additional metrics.

TIME SYNCHRONISATION

Synchronisation of nodes has to be maintained for collaborative processing of nodes. These are needed for sensing tasks, scheduling of nodes, tracking of objects in network, access control of channel based on time division, aggregation of data and authentication of the originating node. The available mechanisms are not applicable for hostile networks where security is important. Time synchronisation schemes are prone to various attacks.

TRUST MANAGEMENT SYSTEMS (TMS)

A TMS is useful for WSN for determining the behaviour of a sensor node. Further, it can be used as decision making node. As trustworthiness of node is essential, these managements has to be designed with high constraints. The nodes must be capable to react to various situations.
Different kind of trust methods required for WSN. Although this system is useful to secure from vulnerabilities, it has few issues at the design stage and requires to be noted.

- The TMS must be capable of reacting and withstand several conditions such as decentralisation of BS, node compromises and so on.
- It must be essential to realise several different trust values for distinctive actions of the sensor node.
- The sensor node should have knowledge about its neighbour.
- For maintaining purposes at the BS, the decisions made by the nodes has to be reported to it.
- The overhead implied on a sensor node due to TMS has to be handled.

OTHER SECURITY ISSUES

The security issues other than the ones mentioned above are Survivability, End-to- end security, Support for privacy of nodes in data centric networks (DCS), assessment on security-energy, assurance to data and distribution in case of node compromisation.

The characteristics of the network such as failure of nodes, limitation of batter power, node compromise, unreliability in wireless media. The available approaches are not sufficient and more findings are required in these fields.

CONCLUSION

WSN being an emerging trend for applications, the security of the network is a major concern. Many protocols has been designed for the betterment of sensor applications. However, these protocols fails to secure the data in most of the cases. The significant characteristics of WSN makes it challenging to develop high level security protocols thereby retaining low overheads in network. Various types of attacks on layers of the sensor network has be surveyed and the relevant issues in security were discussed in this paper.

REFERENCES

[1] Yang H, Ricciato F, Lu S, Zhang L. Proc IEEE 2006;94(2):442-54.
[2] Zhou Y, Fang Y, Zhang Y. Communications Surveys & Tutorials IEEE 2008;10(3):6-28.
[3] Wang Y, Attebury G, Ramamurthy B. A survey of security issues in wireless sensor networks. 2006.
[4] López J, Zhou J. Wireless sensor network security: Ios Press; 2008.
[5] Shah RC, Rabaey JM, editors. Energy aware routing for low energy ad hoc sensor networks. Wireless Communications and Networking Conference, 2002 WCNC2002 2002 IEEE; 2002: IEEE.
[6] Ganesan D, Cerpa A, Ye W, Yu Y, Zhao J, Estrin D. J Parallel Distrib Comp 2004;64(7):799-814.
[7] Hill JL. System architecture for wireless sensor networks: University of California, Berkeley; 2003.
[8] Ilyas M, Mahgoub I. Handbook of sensor networks: compact wireless and wired sensing systems: CRC press; 2004.
[9] Shi E, Perrig A. Wireless Communications IEEE 2004;11(6):38-43.

[10] Qian Y, Lu K, Tipper D, editors. Towards Survivable and Secure Wireless Sensor Networks. Performance, Computing, and Communications Conference, 2007 IPCCC 2007 IEEE Internationa; 2007: IEEE.
[11] Qian Y, Lu K, Tipper D. Wireless Comm IEEE 2007;14(5):30-7.
[12] Kavitha T, Sridharan D. Security vulnerabilities in wireless sensor networks: A survey.
[13] Pathan A, Lee H-W, Hong CS, editors. Security in wireless sensor networks: issues and challenges. Advanced Communication Technology, 2006 ICACT 2006 The 8th International Conference; 2006: IEEE.
[14] Xiao M, Wang X, Yang G, editors. Cross-layer design for the security of wireless sensor networks. Intelligent Control and Automation, 2006 WCICA 2006 The Sixth World Congress on; 2006: IEEE.
[15] Zia T, Zomaya A, editors. Security issues in wireless sensor networks. Systems and Networks Communications, 2006 ICSNC'06 International Conference on; 2006: IEEE.
[16] Law YW. Key management and link-layer security of wireless sensor networks: Energy-efficient attack and defense. 2005.
[17] Shaikh RA, Lee S, Song YJ, Zhung Y, editors. Securing distributed wireless sensor networks: issues and guidelines. Sensor Networks, Ubiquitous, and Trustworthy Computing, 2006 IEEE International Conference on; 2006: IEEE.
[18] Raymond DR, Midkiff SF. Pervasive Computing IEEE 2008;7(1):74-81.
[19] Saxena M. Security in wireless sensor networks-a layer based classification. Department of Computer Science, Purdue University. 2007.
[20] Yi Yang, Xinran Wang, Sencun Zhu, and Guohong Cao. Distributed Software-based Attestation for Node Compromise Detection in Sensor Networks, 26th IEEE International Symposium on Reliable Distributed Systems, IEEE Computer Society, PP: 219 – 228, 2007.
[21] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou. IEEE Communications Surveys & Tutorials 2009;11(2):52 – 73.
[22] Mohammad Nikjoo S, Arash Saber Tehrani and Priyantha Kumarawadu. Secure Routing in Sensor Networks, IEEE, pp. 978 – 981, 2007.
[23] C Karlof and D Wagner. Summary of "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, Seminar on Theoretical Computer Science. 27.4.2005