Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Security in Wireless Sensor Network

Saurabh Kulkarni
Department Of Information Technology, PVPPCOE,Mumbai,India

Abstract — ***Wireless Sensor Network is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance future. The inclusion of wireless communication technology also incurs various types of security threats. However, like any other system, security is one of the important issues in any WSN application. The purpose of this paper is to investigate the security attacks and mechanism that apply to wireless sensor network. It also discusses Trust Management issue that is important in security.***
Keywords- Wireless Sensor Network, Security, Intrusion, Attacks, Trust Management

I. INTRODUCTION

Wireless Sensor Network is composed of large number of sensor nodes that are scattered in harsh environment. This network is like any other network is prone to various security issues. So understanding security of wireless sensor network is important issue. There are so many mechanisms are developed to provide the security to sensor network or node. One of the important issue in security of wireless sensor network is trust management. This paper organized as follows: Section II contain Introduction to wireless sensor network and its security. Section III describes security mechanism that applies to wireless sensor network. Section IV contains classification of security and Section V consists of Trust Management. Section VI concludes the paper.

II. SECURITY IN WIRELESS SENSOR NETWORK

A wireless sensor network is a composed of large number of nodes that are densely deployed either inside the phenomenon or very close to it. It is spatially distributed autonomous devices using sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different locations. Wireless Sensor Network may operate in hostile environment, so security is needed to ensure the integrity and confidentiality of sensitive information. Security is important field in WSNs, which is quite different from traditional security mechanism. This is because of two major reasons. Firstly, there are severe constraints on these devices namely their minimal energy, computational and communicational capabilities. Secondly, there is an additional risk of physical attacks such as node capture and tampering. Sensor networks also introduce severe resource constraints due to their lack of data storage and power. Both of these represent major obstacles to the implementation of traditional computer security techniques in a wireless sensor network.

III. SECURITY MECHANISM

Figure 1 shows two types of mechanism Low level and High level.

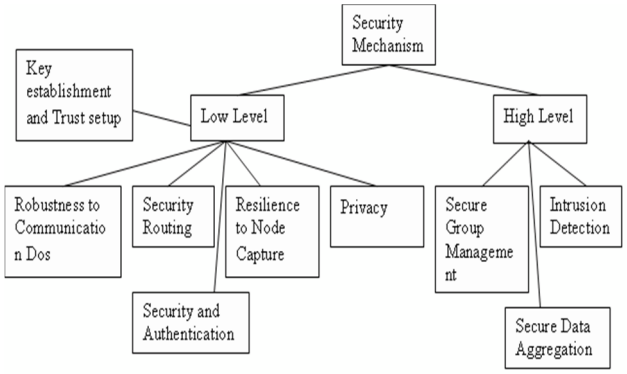

Fig. 1 Security Mechanism

A. Low-Level Mechanism

Low-level security primitives for securing sensor networks includes,

1) Key Establishment And Trust Setup: The primary requirement of setting up the sensor network is the establishment of cryptographic keys. Generally the sensor devices have limited computational power and the public key cryptographic primitives are too expensive to follow. Key-establishment techniques need to scale to networks with hundreds or thousands of nodes. Sensor nodes may need to set up keys with their neighbours and with data aggregation nodes. The disadvantage of this approach is that attackers who compromised sufficiently and many nodes could also reconstruct the complete key pool and break the scheme. [2]

2) Secrecy And Authentication.: Most of the sensor network applications require protection against eavesdropping, injection, and modification of packets. Cryptography is the standard defence. Remarkable system trade-offs arise when incorporating cryptography into sensor networks. For point- to-point communication [8], end-to-end cryptography achieves a high level of security but requires that keys be set up among all end points and be incompatible with passive participation and local broadcast. Link-layer cryptography with a network wide shared key simplifies key setup and supports passive participation and local broadcast, but intermediate nodes might eavesdrop or alter messages.

3) Privacy: Like other traditional networks, the sensor networks have also force privacy concerns.

4) Robustness To Communication Denial Of Service: An adversary attempts to disrupt the network's operation by broadcasting a high-energy signal. If the transmission is powerful enough, the entire system's communication could be jammed.

5) Secure Routing: Routing and data forwarding is a crucial service for enabling communication in sensor networks. Unfortunately, current routing protocols suffer from many security vulnerabilities. For example, an attacker might launch denial of- service attacks on the routing protocol, preventing communication. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies.

6) Resilience To Node Capture: One of the most challenging issues in sensor networks is resiliency against node capture attacks. In most applications, sensor nodes are likely to be placed in locations easily accessible to attackers. Such exposure raises the possibility that an attacker might capture sensor nodes, extract cryptographic secrets, modify their programming, or replace them with malicious nodes under the control of the attacker. Tamper-resistant packaging may be one defence, but it's expensive, since current technology does not provide a high level of security. Algorithmic solutions to the problem of node capture are preferable. [2]

B. High-Level Mechanism

1) Secure Group Management: Each and every node in a wireless sensor network is limited in its computing and communication capabilities. However, interesting in-network data aggregation and analysis can be performed by groups of nodes. Consequently, secure protocols for group management are required, securely admitting new group members and supporting secure group communication. The outcome of the group key computation is normally transmitted to a base station. The output must be authenticated to ensure it comes from a valid group. [2]

2) Secure Data Aggregation: The sensed values must be aggregated to avoid overwhelming amounts of traffic back to the base station. For example, the system may average the temperature of a geographic region, combine sensor values to compute the location and velocity of a moving object, or aggregate data to avoid false alarms in real-world event detection. Depending on the architecture of the wireless sensor network, aggregation may take place in many places in the network. All aggregation locations must be secured. [3]

3) Intrusion Detection: Intrusion detection as it applies to detecting attacks on the sensor network itself, rather than the popular intrusion detection application being researched for such uses as perimeter monitoring, and so forth. Wireless sensor networks are susceptible to many forms of intrusion.

IV. CLASSIFICATION OF SECURITY

We classify the main aspects of wireless sensor network security into three major categories: the obstacles to sensor network security, the requirements of a secure wireless sensor network, attacks.

A. Obstacles Of Sensor Security

To develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to

know and understand these constraints first.

B. Very Limited Resources

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor.

C. Limited Memory and Storage Space

A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

D. Power Limitation

Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network. When adding security to a sensor node, we are interested in the impact that security has on the lifespan of a sensor. The extra power consumed by sensor nodes due to security is related to the processing required for security functions (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead, and the energy required to store security parameters in a secure manner.

E. Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication.

F. Unreliable Transfer

Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. Higher channel error rate also forces the software developer to devote resources to error handling.

G. Conflicts

Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem.

H. Latency

The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes.

I. Unattended Operation

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes that describe below:

J. Exposure to Physical Attacks

The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network.

K. Managed Remotely

Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance

issues. Perhaps the most extreme example of this is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed.

L. No Central Management Point

A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

M. Security Requirements

We can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks.

N. Data Confidentiality

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following:

A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive. In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network. Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

O. Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

P. Data Freshness

Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared- key strategies employed in the design. Typically shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time. To solve this problem a nonce, or another time-related counter, can be added into the packet to ensure data freshness. Availability Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. But all these approaches weaken the availability of a sensor and sensor network for the following reasons:

Additional computation consumes additional energy. If no more energy exists, the data will no longer be available. Communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict. A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network.

Q. Self-Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations.

R. Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor's radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to- end delay of a packet as it travels

between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc.

S. Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate no secured location information by reporting false signal strengths, replaying signals, etc.

T. Authentication

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

U. Attacks

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on. Wireless Sensor networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Figure 2 shows the classification of attacks under general categories and Figure 3 shows the classification of attacks on WSN. Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms).Security mechanism describe above now attacks on routing mechanism.

1) *Passive Attacks: The* monitoring and listening of the communication channel by unauthorized attackers are known as passive attack. The Attacks against privacy is passive in nature.

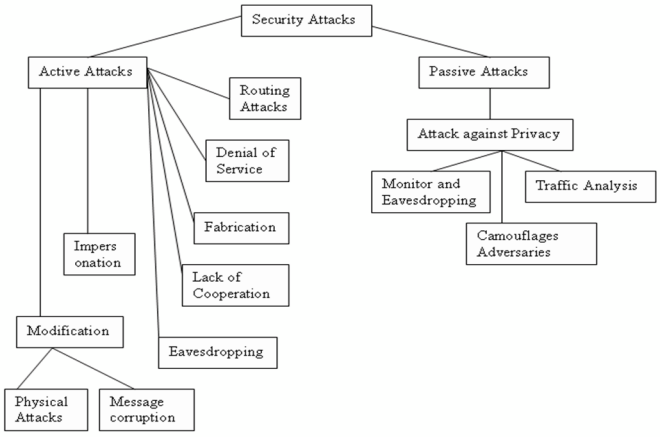

Fig. 2. General Classification of Security Attacks

2) *Attacks against Privacy:* The main privacy problem is not that sensor networks enable the collection of information. In fact, much information from sensor networks could probably be collected through direct site surveillance. Rather, sensor networks intensify the privacy problem because they make large volumes of information easily available through remote access. Some of the more common attacks [4] against sensor privacy are:

a) *Monitor and Eavesdropping:* This is the most common attack to privacy. By snooping to the data, the adversary could easily discover the communication contents. When the traffic conveys the control information 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.

b) *Traffic Analysis:* Even when the messages transferred are encrypted, it still leaves a high possibility analysis of the communication patterns. Sensor activities can potentially reveal enough information to enable an adversary to cause malicious harm to the sensor network.

c) *Camouflage Adversaries:* One can insert their node or compromise the nodes to hide in the sensor network. After that these nodes can copy as a normal node to attract the packets, then misroute the packets, conducting the privacy analysis. The unauthorized attackers monitors, listens to and modifies the data stream in the communication channel are known as active attack. The following attacks are active in nature.

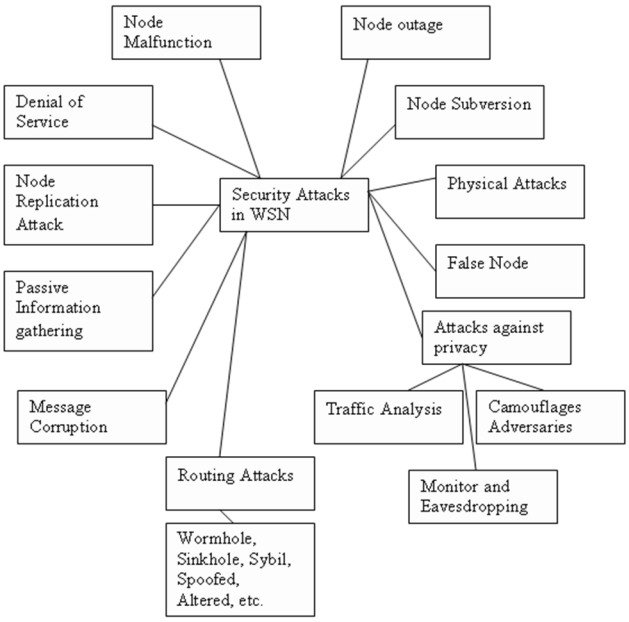

Fig. 3. Classification of Security Attacks on WSN

3) *Active Attacks*

a) Routing Attacks in Sensor Networks: The attacks which act on the network layer are called routing attacks. The following are the attacks that happen while routing the messages.

b) *Spoofed, altered and replayed routing information:* An unprotected ad hoc routing is vulnerable to these types of attacks, as every node acts as a router, and can therefore directly affect routing information. Create routing loops, Extend or shorten service routes. Generate false error messages, Increase end-to-end latency [5]

c) *Selective Forwarding:* A malicious node can selectively drop only certain packets. Especially effective if combined with an attack that gathers much traffic via the node. In sensor networks it is assumed that nodes faithfully forward received messages. But some compromised node might refuse to forward packets, however neighbours might start using another route. [5]

d) *Sybil Attack:* In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes (Figure 4). This type of attack where a node forges the identities of more than one node is the Sybil attack. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehaviour detection.

Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

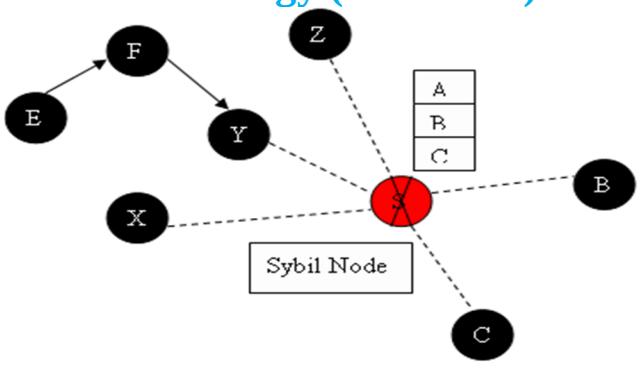

Fig. 4. Sybil Attack

e) *Black hole/Sinkhole Attack:* In this attack, a malicious node acts as a black hole to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes, it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations. Figure 5 shows the conceptual view of a black hole/sinkhole attack.

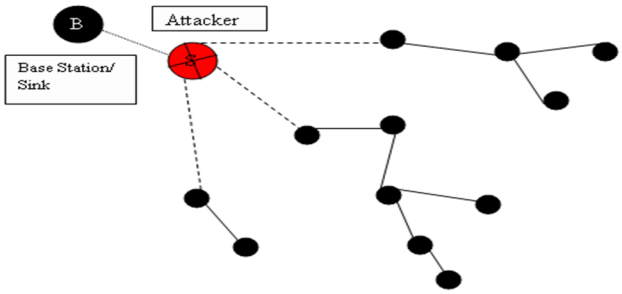

Fig. 5. Black hole/Sink hole Attack

f) *Hello Flood Attack:* Hello Flood Attack is introduced. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission (termed as a laptop-class attacker in [5]) range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbour. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbour and are ultimately spoofed by the attacker.

g) *Wormhole Attack:* Wormhole attack is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. The tunnelling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighbouring information. Figure 6 shows a situation where a wormhole attack takes place. When a node B (for example, the base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighbourhood. Each neighbouring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as its parent. Hence, even if the victim nodes are multi hop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole.

Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

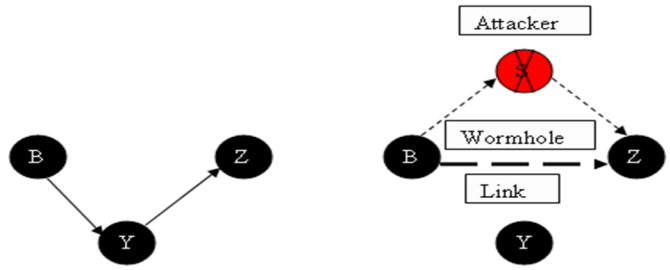

Fig. 6. Worm hole Attack

h) *Denial of Service:* The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. 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. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and resynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

i) *Node Subversion:* Capture of a node may reveal its information including disclosure of cryptographic keys and thus compromise the whole sensor network

j) *Node Malfunction:* A malfunctioning node will generate inaccurate data that could expose the integrity of sensor network especially if it is a data-aggregating node such as a cluster leader [3].

k) *Node Outage:* Node outage is the situation that occurs when a node stops its function. In the case where a cluster leader stops functioning, the sensor network protocols should be robust enough to mitigate the effects of node outages by providing an alternate route [3].

l) *Physical Attacks:* Sensor networks typically operate in hostile outdoor environments. In such environments, the small form factor of the sensors, coupled with the unattended and distributed nature of their deployment make them highly susceptible to physical attacks, i.e., threats due to physical node destructions. Unlike many other attacks mentioned above, physical attacks destroy sensors permanently, so the losses are irreversible. For instance, attackers can extract cryptographic secrets, tamper with the associated circuitry, modify programming in the sensors, or replace them with malicious sensors under the control of the attacker.

m) *Message Corruption:* Any modification of the content of a message by an attacker compromises its integrity. [6]

n) *False Node:* A false node involves the addition of a node by an adversary and causes the injection of malicious data. An intruder might add a node to the system that feeds false data or prevents the passage of true data. Insertion of malicious node is one of the most dangerous attacks that can occur. Malicious code injected in the network could spread to all nodes, potentially destroying the whole network, or even worse, taking over the network on behalf of an adversary. [6]

o) *Node Replication Attacks:* Conceptually, a node replication attack is quite simple; an attacker seeks to add a node to an existing sensor network by copying the node ID of an existing sensor node. A node replicated in this approach can severely disrupt a sensor network's performance. Packets can be corrupted or even misrouted. 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. [2]

p) *Passive Information Gathering:* An adversary with powerful resources can collect information from the sensor networks if it is not encrypted. An intruder with an appropriately powerful receiver and well-designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of

messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used. [4]

q) *Attacks on Information in transit:* In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate packets thus, provide wrong information to the base stations or sinks.

r) *Information Flooding:* In [1], the randomized data routing mechanism and phantom traffic generation mechanism are used to disguise the real data traffic, so that it is difficult for an adversary to track the source of data by analysing network traffic.

s) Baseline Flooding: In the baseline implementation of flooding, every node in the network only forwards a message once, and no node retransmits a message that it has previously transmitted. When a message reaches an intermediate node, the node first checks whether it has received and forwarded that message before. If this is its first time, the node will broadcast the message to all its neighbours. Otherwise, it just discards the message.

t) *Probabilistic Flooding:* In probabilistic flooding, only a subset of nodes within the entire network will participate in data forwarding, while the others simply discard the messages they receive. One possible weakness of this approach is that some messages may get lost in the network and as a result affect the overall network connectivity. However, as explain later in this section, this problem does not appear to be a significant factor.

u) *Flooding with Fake Messages:* The previous flooding strategies can only decrease the chances of a privacy violation. An adversary still has a chance to monitor the general traffic and even the individual packets. This observation suggests that one approach to alleviate the risk of source-location privacy breaching is to augment the flooding protocols to introduce more sources that inject fake messages into the Network. By doing so, even if the attacker captures the packets, he will have no idea whether the packets are real.

v) *Phantom Flooding:* Phantom flooding shares the same insights as probabilistic flooding in that they both attempt to direct messages to different locations of the network so that the adversary cannot receive a steady stream of messages to track the source. Probabilistic flooding is not very effective in achieving this goal because shorter paths are more likely to deliver more messages. Therefore, suggest enticing the attacker away from the real source and towards a fake source, called the phantom source. In phantom flooding, every message experiences two phases: (1) a walking phase, which may be a random walk or a directed walk, and (2) a subsequent flooding meant to deliver the message to the sink. When the source sends out a message, the message is unicast in a random fashion within the first hwalk hops (referred to as random walk phase). After the hwalk hops, the message is flooded using the baseline flooding technique (referred to as flooding phase).

V. TRUST MANAGEMENT

Trust is an old but important issue in any networked environment, whether social networking or computer networking. Trust can solve some problems beyond the power of the traditional cryptographic security. For example, judging the quality of the sensor nodes and the quality of their services, and providing the corresponding access control, e.g., does the data aggregator perform the aggregation correctly? Does the forwarder send out the packet in a timely fashion? These questions are important, but difficult, if not impossible, to answer using existing security mechanisms. We argue that trust management is the key to build trusted, dependable wireless sensor network applications. However, it is not easy to build a good trust model within a sensor network given the resource limits. Furthermore, in order to keep the sensor nodes independent, we should not assume there is a trust among sensors in advance. Trust management schemes are classified into three categories: centralized, distributed and hybrid as shown in Figure 7. Centralized trust management (CTM) schemes consist of a single globally trusted server that determines the trust values of every node in the network. This gives the benefit of lesser computational overhead at the sensor node because most of the trust calculation is performed at centralized trusted server that has no constraints of computational power and memory. This approach however has the drawbacks of a single point of failure, which makes it least reliable. Also, it suppresses the underlying fact that different nodes may have different trust values about a particular given node. For large scale sensor networks, centralized trust schemes are not suitable because the total routing cost for the exchange of trust values of a sensor node with the base station is quite energy expensive, especially when the base station is located far from the node. Therefore centralized approach introduces large communication overhead in the sensor network.

Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

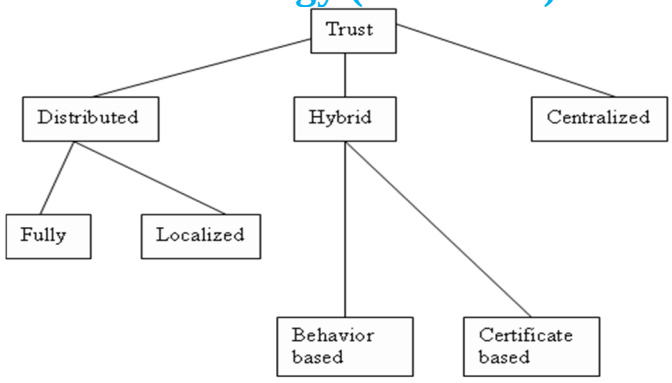

Fig. 7. Taxonomy of Trust

Distributed trust management (DTM) schemes also do not work well for large-scale sensor networks. In the distributed approach, every node locally calculates the trust values of all other nodes in the network that increases the computational cost. Also each node needs to maintain an up-to-date record about the trust values of the entire network in the form of a table. The size of the table is directly proportional to the size of the network which results in a large memory consumption. Each sensor node maintains its own trust record and that gives the benefit of less Communication overhead because a node does not need to contact with some centralized server.

The distributed approach is more reliable than the centralized one because it has no single point of failure. In the wireless sensor network domain, some researchers use restricted DTM approach, in which sensor nodes only maintains the trust value about its neighbouring nodes only. We refer to that approach as a localized DTM approach and the earlier one as a fully DTM approach. The major drawback of the localized DTM approach is that it introduces delay and dependency whenever any node wants to evaluate trust of distant nodes. This is due to the fact that trust is established "dynamically at runtime using the chain of trust relationships between neighbouring nodes".

Hybrid trust management (HTM) schemes contain the properties of both centralized as well as distributed trust management approaches. The main objective of this approach is to reduce the cost associated with trust evaluation as compared to distributed approaches. This scheme is used with clustering schemes, in which cluster- head acts as a central server for the whole cluster. This approach is more reliable than the centralized one but less reliable than the distributed one. For intra-cluster communication, nodes need to contact the cluster head. It introduces more communication overhead in the network as compared to the distributed one. The advantages and disadvantages of all three approaches are summarized in Table 1. All these three trust management approaches are further classified into two categories: certificate-based trust management approach and behaviour-based trust management approach. In the certificate-based trust management approach, trust is mainly based on the provision of a valid certificate assigned to a target node by a centralized certification authority or by other trusted issuer. In the behaviour-based trust management approach, an entity calculates the trust values by continuous direct or indirect monitoring of other nodes. Table 2 gives the classification of proposed trust management schemes of wireless sensor networks based on our proposed trust taxonomy.

Reputation based Framework for Sensor Network (RFSN) where each sensor node maintains the reputation for neighbouring nodes. On the basis of that reputation trust values are calculated. The RFSN scheme follows the localized distributed approach and borrows some design features from several existing works in the literature.

The Agent based Trust and Reputation Management (ATRM) scheme for wireless sensor networks. The ATRM is based on a clustered wireless sensor networks and calculates trust in a fully distributed manner. Every sensor node holds a local mobile agent that is responsible for administrating trust and reputation of hosting node. ATRM assumes that there is a trusted authority which is responsible for generating and launching mobile agents. It also assumes that mobile agents are resilient against malicious nodes that try to steal or modify information carried by the agent. The major advantage of the ATRM scheme is that they use mobile agents for trust calculation which reduces the bandwidth consumption and time delay.

Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

TABLE 1. ADVANTAGES AND DISADVANTAGES OF TRUST MANAGEMENT APPROACHES

	Advantages	Disadvantages
Centralized	•Least computational Overhead. •Least memory usage.	•Least reliable (Single point of failure). •Most communication overhead.
Distributed	•Most Reliable (no Single point of failure). • Scalable.	•Most computational Overhead. •Most memory usage.
Hybrid	•Less Communication overhead than centralized. •Less memory consumption than distributed. •Less computational overhead than distributed. •More reliable and scalable than centralized.	•Large Computational overhead then centralized. •Large memory requirement than centralized. •Less scalable and reliable than distributed.

Parameterized and Localized trust management Scheme (PLUS) for sensor networks security. The authors adopt a localized distributed approach and trust is calculated based on either direct observations or indirect observations. Trust calculation mechanism involves the combination of six parameters: 1) ordering, 2) integrity checking, 3) confidentiality checking, 4) responsibility checking, 5) positivity checking and 6) cooperative checking. The involvement of so many parameters makes this scheme less generic and more complex.

TABLE 2. APPLICATION OF TRUST TAXONOMY

		Certificate- based	Behavior- based
Centralized		-	-
Hybrid		-	GTMS [Group-based trust management scheme]
		-	
Distributed	Fully	ATRM [Agent based Trust and Reputation Management]	-

Volume 3 Issue IX, September 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

	Localized	-	PLUS [Parameterized and Localized trust management Scheme] , RFSN [Reputation based Framework for Sensor Network] , T-RGR [trust management scheme for Resilient Geographic Routing]

Simple trust management scheme for Resilient Geographic Routing (T-RGR) scheme. Their trust algorithm works in a localized distributed manner, in which each node monitors the behaviour of the one-hop neighbours. If neighbouring node successfully forwards the packet it will increase the trust value by a constant parameter, and if it drops the packet then the source node will decrease its trust value by another constant parameter. If the trust value of a particular node is greater than the predefined threshold value, then the node will be considered as a trusted node, otherwise it will be un-trusted.

Group-based trust management scheme (GTMS) for clustered wireless sensor networks. The unique thing about the GTMS scheme is that in contrast to traditional trust management approaches, which always focus on trust values of individual users, the GTMS scheme evaluates the trust of a group of users. That group based approach gives the benefit of less memory consumption. GTMS calculate the trust value based on direct or indirect observations. Direct observations represent the number of successful and unsuccessful interactions and indirect observations represent the recommendations of trusted peers about a specific node.

IV. CONCLUSION

In this paper, I have presented the general concept of wireless sensor network and security in wireless sensor network. Current research so far focuses on the security of wireless sensor network. There is various mechanism of security that applies in our network so our network is more prone to failure. I have also described many attacks that occur in sensor network and also apply to sensor node. Additionally, the most important issue in security is Trust management is also described. In future, so many attacks will be introduced that are harm the sensor network and sensor node, mechanism to prevent it.

REFERENCES

[1] John Paul Walters, Zhengqiang Liang, Weisong Shi, and Vipin Chaudhary Department of Computer Science Wayne State University Wireless Sensor Network Security: A Survey. Auerbach Publications, CRC Press 2006
[2] Adrian Perrig, John Stankovic, David Wagner, “Security in Wireless Sensor Networks” Communications of the ACM, Page53-57, year 2004
[3] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, “Security in wireless sensor networks: issues and challenges” Advanced Communication Technology (ICACT), Page(s):6, year 2006
[4] Undercoffer, J., Avancha, S., Joshi, A. and Pinkston, J. “Security for sensor networks”. In Proceedings of the CADIP Research Symposium, University of Maryland, Baltimore County, USA, year 2002
[5] Chris Karlof, David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures”, AdHoc Networks (elsevier), Page: 299-302, year 2003
[6] Zia, T.; Zomaya, A., “Security Issues in Wireless Sensor Networks”, Systems and Networks Communications (ICSNC) Page(s):40 – 40, year 2006