Challenges and Authentication in Wireless Sensor Networks by using promising Key Management Protocols

Neethu Myshri R
Lecturer/CSE,
Jain University, Bangalore

A. Jayanthiladevi
Assistant Professor/MCA
Jain University, Bangalore

T. Lalitha, Ph.D
Assistant Professor (Sr)/MCA
Sona College Technology, Salem

ABSTRACT
A network comprising of several minute wireless sensor nodes which are organized in a dense manner is called as a Wireless Sensor Network (WSN). Fig.1 demonstrates the architecture of wireless sensor networks. Every node estimates the state of its surroundings in this network. The estimated results are then converted into the signal form in order to determine the features related to this technique after the processing of the signals. Based on the multi hop technique, the entire data that is accumulated is directed towards the special nodes which are considered as the sink nodes or the Base Station (BS). The user at the destination receives the data through the internet or the satellite via gateway. The use of the gateway is not very necessary as it is reliant on the distance between the user at the destination and the network [1].Usually; the sensor network consists of a huge group of distributed minimum power sensors disseminated over the area which is to be supervised. The sensors possess the capability of collecting the data, processing and then forwarding it to the central node for additional processing [2].The applications of WSNs include environmental monitoring, health, surveillance, catastrophe monitoring, structural monitoring, security, military, industry, agriculture, home, traffic monitoring, etc.When the sensor network is deployed in the battlefield, every data from sink node, reports of every data from sensor nodes to central node, message swapped between sensor nodes need to be encrypted for safeguarding the message from probable eavesdroppers [2].For supervising the physical world, the wireless sensor networks are the promising technology. In order to collect the data from the surrounding in a sensor network application, several minute sensor nodes are organized and collaborated. Sensing modals like image sensors are placed in every node and this possess the ability to communicate in the wireless environment. The major merit of WSN is that it minimizes the application cost by deploying the several sensors with minimum communication cost and with base station offering full network function. [3].

Keywords
Senor, Key, Wireless, Security, Protocols

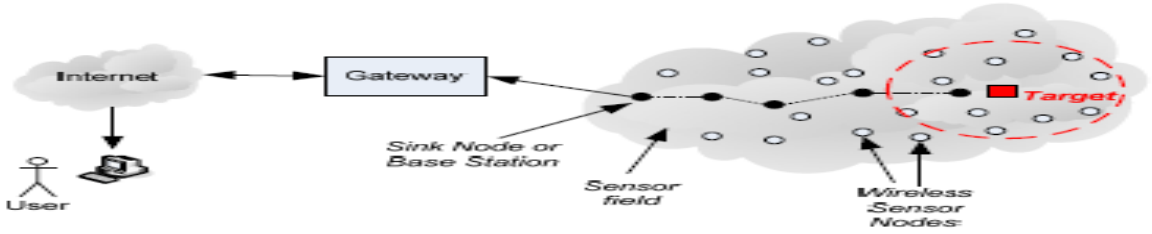

Figure 1: Architecture of wireless sensor networks

1. ATTACKS IN SENSOR NETWORKS
The attacks in sensor networks are normally categorized into following types.

Passive/Active: An active adversary prefers to hinder the process in all possible way. For example, altering the forwarded packet, purposely influencing the MAC layer collisions etc., A passive strategy frequently acts as originator of the active one. For example, looking for most efficient disruption of the network.

Insider/Outsider: This is a main perceptive feature. In every security application fields, insider problem prevails which offers a predominant undesirable problem. With the capacity of the insiders, the adversary can result in the latent damage. These issues are addresses by the researchers by considering threshold protocols for secret sharing and aggregating application protocols.

Static/adaptive: In obscure sense, there is a fairly random difference among them. A learning algorithm in a node is considered as static. In a realistic perspective, the capacity of every network to perform learning with respect to its surrounding causes more energy consumption [4].

Spoofed, Altered, or Replayed Routing Information

These types of attacks mainly point towards routing protocol which deals with routing information. Hence by altering the routing information of the routing protocol via malicious code, the complete routing information of the wireless sensor networks can be modified. The possible methods of performing this action are repeating routing information, limiting or lengthening the routes, spoofing the bogus messages, modifying the loops of routing, or enhancing the end-to-end delay in fig.2.

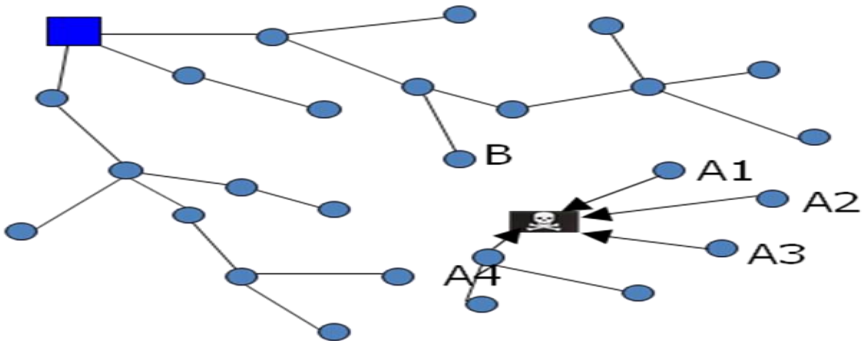

Fig.2.Example: captured node attracts traffic by advertising shortest path to sink, high battery power, etc

Selective Forwarding

The attacker attacks on one of the nodes and corrupt it using a malicious code. This node pretends to be normal node in WSN except that it drops the packets than forwarding the node in the path to the next node which means that it becomes the ineffective node.

Sinkhole Attacks

The main goal of the sink hole attacks is to excite all nodes in close proximity to builds a symbolic sink hole. For example, when one main coordinator is infected by the sink hole, every other node also drops into the sink hole subsequently. This attack gathers every attacking node to be viewed as ideal node for intending the neighboring nodes.

Sybil Attacks

During Sybil attack, the attacker corrupts a single node in the WSN network using malicious code covered with multiple characteristics. Subsequently this single node acts a main delay for the whole sensor network that further decreases the efficiency of fault tolerance techniques such as multi-path routing, upholding topology, etc.

Wormholes

In this type of attacks, the malicious node scoops the messages it received at one end of the network on a separate minimum-latency channel. After that, it reiterates the message at various points in the sensor network. Typically the wormhole attacks employ two different and distant malicious nodes for reducing the isolation from each other by repeating next to an out-of-reach channel which is just present in the attacker refer fig.3.

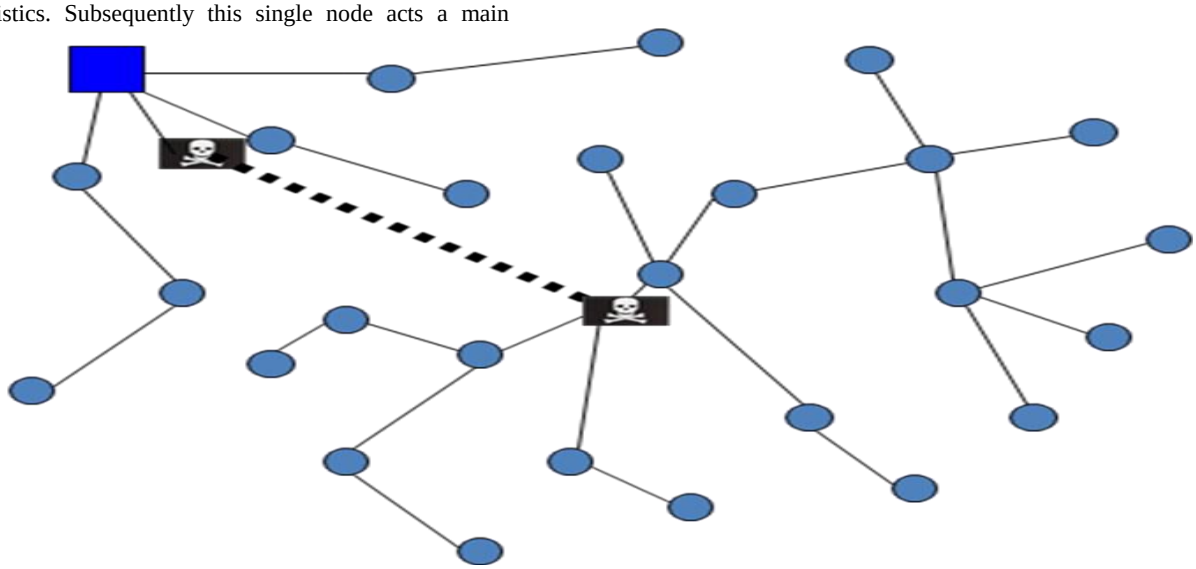

Fig.3.Attacker may influence network topology by delivering routing information to the nodes before it would really reach them by multi hop routing

HELLO Flood Attacks

In several cases, the routing protocols in WSN needs nodes to distribute hello messages to declare themselves to their neighbors. Those nodes that obtain the message believe that it is within the radio range of the sender. But in some cases, this belief may be wrong. Since there is possibility that a lap-top class attacker broadcasting routing with more transmission power proves all other nodes that its neighbor is its attacker. It is not essential for the attacker to build justifiable traffic for using hello flood attack. It can just re-distribute the overhead packets with appropriate power to be gained by the every other node in the network.

Acknowledgement Spoofing

The numerous sensor network routing algorithms depend on implicit or explicit link layer acknowledgements. An adversary will be capable of spoofing link layer acknowledgements owing to the inbuilt broadcast medium, intended for overhead packets addressed to neighboring nodes. The main goal of this attack is to make the sender belief that weak link to be strong or that a dead or disabled node to be alive.

2. NETWORK SECURITY IN SENSOR NETWORKS

In wireless channels, the communication is not completely secure and is subjected to security hazard. In the wireless channels, the possible security threat can be divided into two threats: inside threat and outside threat. In case of outside threat in the sensor network, the attacker does not possess control over the cryptographic materials. Whereas in case of the inside threat, the attacker will be possess some key materials and trust of some sensor nodes.

Compromising the sensor nodes is an easy task due to the absence of the expensive tampering resistant hardware. Even if it possesses the tampering resistant hardware, it may be very reliant. Modification, forging and discarding the messages is possible in case of a compromised node [5].

In vulnerable locations, maintaining the security of the sensor nodes is a major task. In WSN, the encoding and the authentication of the communication carried out is necessary, to ensure security. For communication between the sensor nodes, few solutions have been developed to attain stability in communication. Distribution key method, dissymmetric encryption method, and key predisposition method are the three kinds of key management techniques.

The attacks like jamming and spoofing are very destructive to the sensor networks. Whenever the cluster heads are responsible for the transmission and reception of the data, this nature of the promising key distribution networks makes it susceptible to destructive networks. So, the network will get destructed if a hacker tries to become the cluster head of the cluster. Examples of this type of attack are the selective forwarding and the sinkhole attacks.

3. KEY MANAGEMENT IN WIRELESS SENSOR NETWORKS

Use of the pair wise keys between sensor nodes is the necessary requirement of the WSN for ensuring security. The trusted-server scheme, the self-enforcing scheme, and the key pre distribution scheme are the three classes of the key agreement schemes. A trusted server is assumed to exist in the case of trusted-server scheme for the establishment of keys between the nodes. But in case of distributed sensor networks, trusted server scheme is not appropriate due to the difficulty in developing a trusted network. Asymmetric cryptography, like that of public key certificate is utilized in the self enforcing scheme. But for sensor networks, use of the public key algorithm is inappropriate due to the restricted amount of power and resources for computation in the minute sensor node. In the key pre-distribution schemes, loading of the keying materials takes place at a prior basis in the sensor nodes [6].In a wireless sensor network, the computation and communication capacity of every node is limited to a particular level. Node groups can be used for executing in network data aggregation and analysis. Refer fig.4.For instance, a vehicle can be tracked by a node group jointly via network. The nodes belonging to a group will keep varying repeatedly and at a faster rate in the network. In the wireless sensor network, most of the key services are executed by the groups. Hence, for admission of the new members to the group and to support group communication at a secure level, it is necessary to have a secure protocol for group management. After the computation within the group, the result is transferred to the base station. In order to ensure the transmission from a legitimate group, the result must be authenticated .More often the usage of the sensor network is in environment which is open and not well monitored. Key management has become a challenging task due to the numerous sensor nodes used and the reduced knowledge about the sensor node deployment abilities Impracticality of public key cryptosystems: The usage of the public-key algorithms, like that of Diffie-Hellman key agreement or RSA signatures is not desired due to the restricted ability of computation and restricted availability of the power resources in the sensor nodes. At present, the operations are executed by the sensor nodes over a time interval of seconds to minutes thus making it more prone to t he threats like denial of service (DoS) attacks in the network. Limited memory resources: Due to the limited memory of the sensor nodes, the key storage memory is also limited. Hence it is not possible to assign unique keys to each node in this network.

4. AUTHENTICATION IN SENSOR NETWORKS

The secured communication can be realized using user authentication concept. This constitutes three phases that are described as follows

1. Registration Phase: The user ID and password of the user is submitted to gateway node.

2. Login Phase: The user ID and password is submitted to the login node.

3.Authentication Phase: The user and timestamp's validity is verified by the gateway node [7].
The public key cryptography is used when there is large number of user due to its scalability. Since public key cryptography is more power consuming sensor communicates among each other with the help of symmetric cryptography. Thus the sensors in the communication range serve as promoters between public key cryptography of the user and symmetric crypto world of WSN. The user communicates to sensors with the help of public key cryptography and sensors communicate to the rest of the sensor network using symmetric cryptography and this process occurs in authenticate manner as follows.

5. PROMISING KEY MANAGEMENT PROTOCOLS

This protocol is simple, elegant and provides effective tradeoff between robustness and scalability.
In this scheme a large pool of keys are generated (eg: 10,000 keys), randomly take 'K' keys out of the pool to establish a key ring (K << N).

Path Key Discovery: When two nodes communicate they search for a common key within the key ring by broadcasting their identities (ID's) of the keys they have.

5.1. Key Ring and Key Pool Size

Due to the limited communication capabilities a number of nodes with which a particular node can communicate is n'<<n.This means that the probability of two nodes sharing at least one key in their key rings of size k is p'=d/(n'-1)>>p

Key pool size P can be derived as a function of k:

$$p' = 1 - \frac{(1-\frac{k}{P})^{2(P-k+1/2)}}{(1-\frac{2k}{P})^{(P-2k+1/2)}}$$

Consequently, the probability that no key is shared between the two rings is the ratio of the number of rings without a match by the total number of rings.

$$\frac{k!(P-k)!(P-k)!}{P!k!(P-2k)!}$$

$$p' = 1 - \frac{(1-\frac{k}{P})^{2(P-k+1/2)}}{(1-\frac{2k}{P})^{(P-2k+1/2)}}$$

5.2. Key Management: Constraints and Simulation Results

Refer Fig 5. For Number of sensors to corrupt in order to compromise an arbitrary channel

- Sensor node constraints:
  - Battery power
  - Transmission range
  - Memory
  - Temper protection
  - Sleep pattern
- Network constraints:
  - Ad-hoc network nature
  - Packet size.

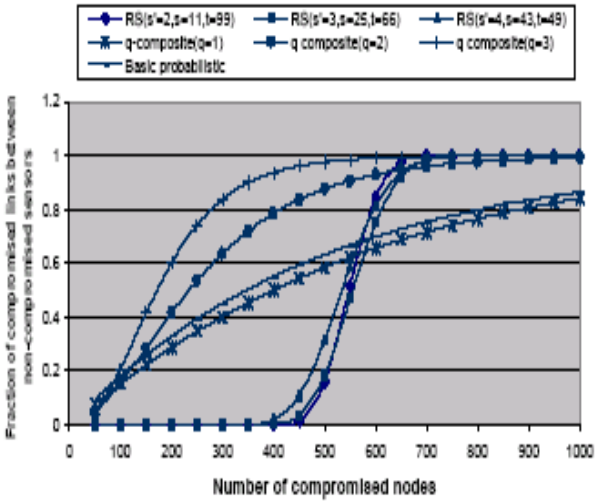

Fig.5. Fraction of compromised links between non compromised nodes vs number of compromised nodes

5.3. Key management: evaluation/comparison metrics

Resilience against node capture: how many nodes are to be compromised in order to affect traffic of not compromised nodes? Addition: how complicated is dynamic node addition? Revocation: how complicated is dynamically node revocation? Supported network size: what is the maximum possible size of the network.

5.4. PERFORMANCE ANALYSIS

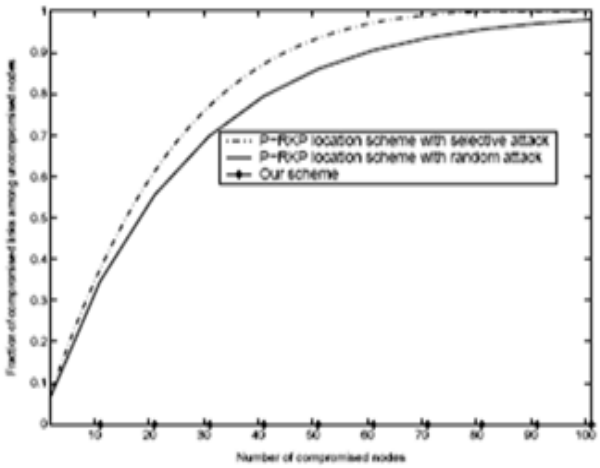

Fig6. Random/Selective Node capture attack v/s promising key management protocol

5.5. Key management approaches classification Approaches

According to the model, network consists of three types of nodes: command node, gateways and regular sensor nodes. Gateways partition the network into distinct clusters as follows as in Fig.7

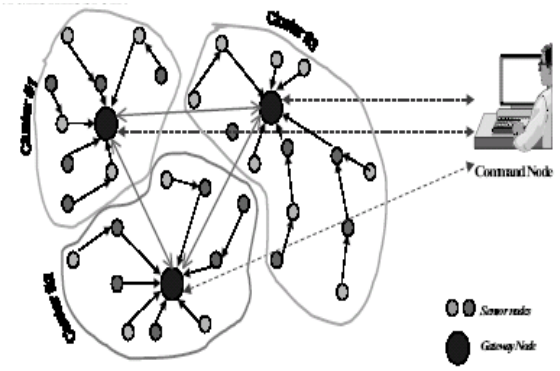

Fig.7. **Gateways partition the network into distinct clusters**

5.6. Key establishment within the same zone

Key establishment within the same zone Each sensor, say [(i,j),b], broadcasts identifier [(i,j),b] and key space identifiers [,] For each neighbor, sensor adds a link in *key-graph* if they share a key .Sensor broadcasts list of neighbors who share key-space with it. Uses similar messages from others to expand key-graph.Source routing to request and establish pair wise keys with all its neighbors.

5.7. Key establishment within adjacent zones

Each sensor, broadcasts desired node list (of nodes in the adjacent zone).A neighbor of the requestor within the same zone who already shares a key with the nodes for each neighbor, sensor adds a link in *key-graph* if they share a key. Sensor broadcasts list of neighbors who share key-space with

it. Uses similar messages from others to expand key-graph. Source routing to request and establish pair wise keys with all its neighbors.

Memory overhead for p = 0.5238, m = 68

Security Analysis Secure against Random Node capture, Selective Node capture and Node Fabrication attacks.

6. CONCLUSION

This paper focuses on the promising key management technique for optimizing overhead and providing authentication in wireless sensor networks. The Key achievements are as follows.

1) Development of promising key based technique for key management in wireless sensor network. This technique allows inter cluster as well as intra network communication in a very efficient manner with high security.

2) Development of promising based key management technique for authentication in wireless sensor network. This technique recovers the compromised nodes in secured manner.

7. REFERENCES

[1] Lina M. Pestana Leão de Brito and Laura M. Rodríguez Peralta, (2008). An Analysis of Localization Problems and Solutions in Wireless Sensor Networks. Polytechnical Studies Review, Vol VI.

[2] D.Saravanan , D.Rajalakshmi and D.Maheswari, (2011), DYCRASEN: A Dynamic Cryptographic Asymmetric Key Management for Sensor Network using Hash Function. International Journal of Computer Applications, Volume 18– No.8.

[3] Mohammed A. Abuhelaleh and Khaled M. Elleithy. (2010). Security in wireless sensor networks: Key management module in SOOAWSN. International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4.

[4] John A. Clark, John Murdoch, John A. McDermid, Sevil Sen, Howard R. Chivers, Olwen Worthington and Pankaj Rohatgi (2007). Threat Modelling for Mobile Ad Hoc and Sensor Networks. In Annual Conference of ITA.

[5] Yingpeng Sang and Hong Shen (2006). Secure Data Aggregation in Wireless Sensor Networks: A Survey (PDCAT).

[6] Jiyong Jang, Taekyoung Kwon and Jooseok Song (2007). A Time-Based Key Management Protocol for Wireless Sensor Networks (ISPEC), pp 314-328

[7] Binod Vaidya, Min Chen and Joel J. P. C. Rodrigues (2009). Improved Robust User Authentication Scheme for Wireless Sensor Networks. Fifth IEEE Conference on Wireless Communication and Sensor Networks(WCSN).