Authentication Techniques for Wireless Sensor Network

Anand D. Dhawale
M.Tech Student Dept. of CSE
Shri. Ramdeobaba Kamla Nehru
College of Engineering Nagpur, Maharashtra.

M. B. Chandak
Head, Department of CSE
Shri. Ramdeobaba Kamla Nehru
College of Engineering Nagpur, Maharashtra

N. V. Thakur
Department of CSE
Shri. Ramdeobaba Kamla Nehru
College of Engineering Nagpur, Maharashtra

ABSTRACT
Wireless sensor networks (WSNs) got high popularity due to broad range of applications. These networks have attracted tremendous researchers due to their unique characteristics that differ them from traditional wired networks. WSNs are special networks having great future ahead but at the same time suffer from many hazards due to their unique characteristics. They are having large number of low cost sensor nodes with low power (usually operated by battery), low processing ability, and communication and storage limitations. The nodes usually called as motes are tiny nodes deployed in target areas. Due to deployment nature and radio links the nodes are easily targeted by attacker with physical attack of node capture. If we think of applying security to WSNs we have to face the resource limitations constraints. The resource limitations don't allow to apply traditional mechanisms having large overhead and computational powers. Out of many security solutions authentication is one of the best solutions to secure the whole network. The network can be made secure if we allow only true information to be inserted from true node. Authentication can be efficiently used to check valid, fake and modified communication. Such authentication techniques in wireless sensor networks are analyzed in this paper and possible solution is suggested in future work.

General Terms
Wireless sensor network, authentication, attacks, security solutions.

Keywords
Wireless Sensor network, attacks, security, authentication.

1. INTRODUCTION
Wireless sensor networks are usually used to monitor environment and have large applications which are sensitive in nature, These applications include monitoring ,controlling and tracking areas like object or human tracking, battlefield monitoring, habitat monitoring. Many of the applications collect and maintain the secured data. The large numbers of sensor nodes are mounted and once deployed there is no manual maintenance and monitoring till long time. Due to this scenario it creates a security problem. Nodes are more likely to be affected by various physical attacks which further cause node compromise, node cloning, man-in-middle attack and replay attack. Lot of researchers are attracted towards the security of wireless sensor network because until no concrete mechanism is established in this case. The reason to this is resource constraint and distributed unattended environment of sensor networks and unattended environment. The research shows that lot of work has been done on the development of wireless sensor networks for application purpose but very little attention is paid for the great security mechanism. Limitations that one may face while applying security mechanism include [2]

- Resource constraints in sensor node.
- Insecure radio links which enable or cause interception or injection of information.
- Deployment of sensor network is usually in hostile environment which can be dangerous with physical attacks.
- Wireless medium don't allow traditional security mechanisms which are best suited for wired medium.

Most of the security mechanisms are not much efficient in wireless sensor networks. It is true that one has to take into account many parameters while applying security solutions. The radio links are easily accessible which add more difficulties. Among many security schemes and mechanism authentication is the most efficient and better solution. Authenticating a node ensures further secure communication through that node. After certain observations it can be stated that some attacks manipulate the nodes of sensor network to introduce malicious "new" nodes. These introduced "new" nodes can be accepted by other normal nodes. So, in this case the authentication protocol is needed to prevent these false nodes. The fig 1 shows key research areas in wireless sensor networks.

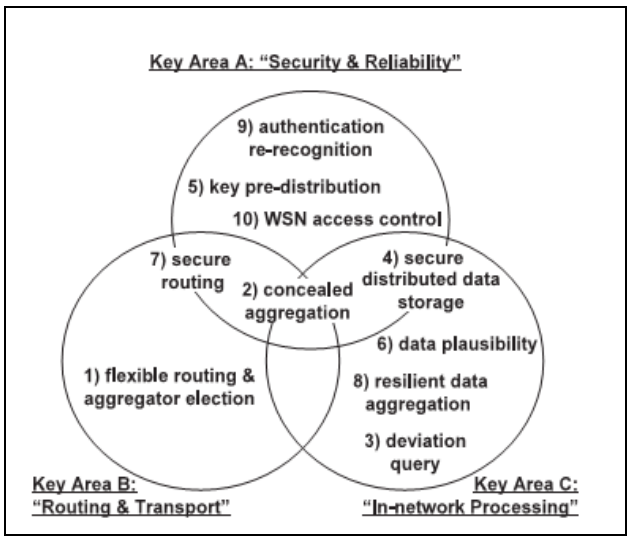

Fig. 1. Key Research areas in WSN

There are different techniques for the authentication:

- All the nodes of sensor network should be authenticated by base station as third party.
- Authentication can be for outsider node, for node to node communication or for node to base station communication.
- Multicast or broadcast authentication is also one of the techniques.
- Authentication of sensor node can be done using clustering method in which cluster head will authenticate other nodes.

2. REVIEW ATTACKS IN WSNs

The small widely spread nodes are susceptible to many kinds of attacks. There are two categories of attacks

- Attacks against basic operation.
- Attacks against security mechanisms.

The different attacks ate on different platforms and use different methodologies.[4]

2.1 Node Capture

The keys and other secured information can be stolen by directly capturing the node with the help of physical attacks. Node capture attacks are the combination of passive, active, and physical attacks usually done by an intelligent attacker. For the sake of initialization or setup an attack, the adversary can gather information about the WSN by eavesdropping on message ex-changes during communication, either local to a using external device. Even if message data are encrypted, the adversary can extract secure information about the network operation, effectively learning about the network structure and function.

2.2 False Node

The fake data can be inserted by the outsider by using false node. This node is the copy of existing node and tries to act as the true node.[1]

2.3 2.3 Malfunctioning of node

The malfunctioning of node can be dangerous because this node injects false information in the network. The whole network might become useless. [1]

2.4 2.4 Sybil Attack

Location based routing protocol is suffered from Sybil attack. In Sybil attack multiple identities of single node are created. The node has to exchange the information with neighbors but can't exchange due to multiple identities of neighbor. If authentication is used then this attack can be prevented. [1]

2.5 2.5 Sinkhole Attack

The traffic of the network is carried out through the compromised node called as sink. The compromised node is made attractive and acts as a powerful node. So, other nodes easily pass data to this sink node and cause network failure.

3. SCENARIO OF APPLYING AUTHENTICATION

Every packet entering in the wireless sensor network must be secured before it is applied for higher level applications. Authentication can be performed in one hop uni-cast, multi-hop uni-cast and broadcast.

3.1 3.1 Authentication with communication pattern

There is certain type of communication in WSNs based upon which authentication techniques are developed.[2]

3.1.1 One-hop authentication

A shared link layer key is required between neighboring nodes. The first implemented architecture providing authentication and encryption is TinySec. Though it is full implantation it does not discuss how to establish link-layer keys.

3.1.2 Multi-hop Authentication

End to end shared keys support multi hop authentication. But it fails if one of the nodes in the path is compromised.

3.1.3 Broadcast Authentication

If source node requires to some message like command it broadcasts the message. In this case each packet which is broadcast should be authenticated so that no false data is inserted.

3.2 Steps Required for Authentication

Before applying authentication technique some prerequisites are there need to complete. The security in wireless sensor network is highly dependent upon the cryptographic keys. The management of these keys is difficult task. The key management is generating, storing, transferring and using the cryptographic keys. Some steps are there to apply:

1. Deployment of network and keys

Network is deployed in the targeted areas and number of keys needed should be calculated.

2. Establishment of keys

Keys are established between nodes which are willing to have the communication.

3. Authentication Protocol

If any node wants to join the network it has to pass some conditions offered by authentication protocol. It is based upon request of the node also.

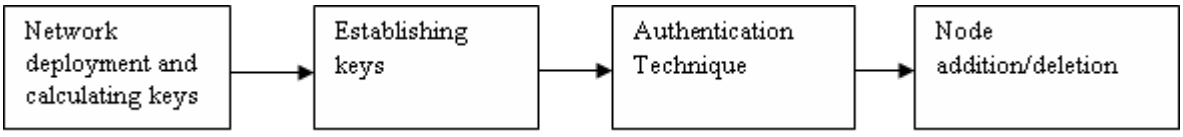

Fig 2. Steps To apply Authentication Technique.

4. Node addition/deletion

The nodes should be added to the network if they are behaving in favor of the applied authentication protocol. It is the responsibility of the authentication protocol to allow node to start secured communication with other member nodes. The malfunctioning or useless nodes should also be deleted by this technique.

4. EXISTING AUTHENTICATION SCHEMES ANALYSIS

There are certain existing authentication schemes in wireless sensor networks. This section analyzes them

4.1 µ TESLA

Micro timed efficient streaming loss tolerant authentication protocol is based upon the broadcasting of packets. The packet is authenticated by key Kmac. Then this key is published. So, no one can be able to get authenticated key details. So, if anyone tries to broadcast the packets before authentication, it will fail. The micro TESLA induces cache delays for broadcast packets. This will create denial of service (DoS) attack. µ TESLA uses a loosely synchronized timer on both the base station and other nodes to authenticate the MAC key . The phases that µ TESLA have are sender setup, broadcasting authenticated packets, bootstrapping a new receiver, and authenticating broadcast packets[3]

4.2 SNEP

This secured network encryption protocol (SNEP) has two entities base station and master key for generation of keys. Each node shares a pair of key with base station and other keys are obtained from master key. It is very useful protocol which guarantees confidentiality and integrity. The only drawback is that it does not handle node capture and DoS attacks effectively. [5]

4.3 Authenticating a message with MAC

The message authentication code (MAC) can be attached to packet while transmitting. If we consider symmetric key technology, the MAC is generated by shared key among sender and receiver. The sender concatenates a message M with key K and calculated MAC C=H(M || K), H() is a hash function. At receiver side packet [M.C} is received. Receiver finds a MAC C' using message M and shared key K. It will check C==C". If it is the case then message is authenticated and it is confirmed that sender is true.

4.4 LEAP

Encryption and Authentication Protocol(LEAP) is used for data switching scheme where nodes having different security requirements. The levels of keys are private keys, pair of keys between node, cluster key and group key. It supports data origin authentication and security for data inside the network. The disadvantage is it fails to provide high security to main nodes like gateways and do not prevent Denial of service attacks. [5]

4.5 Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks

The paper "Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks" by Qiang Huang et. al at Princeton University and Mitsubishi Electric Research Laboratories to create an "efficient authenticated key establishment protocols between a sensor and a security manager in a self organizing network"[4]. In this project the researchers used elliptic curve cryptography (ECC) to provide encryption for the sensor nodes. ECC was chosen because only small key lengths are needed in order to get a reasonable amount of security. To authenticate keys, certificates are used to find out if the public key is in fact a trusted sensor.

4.6 User Authentication

If any user wants to exchange data with sensor nodes, it has to register to base station. The user sends a signed request to other sensor nodes and the nodes verify the request based upon ID of the node. After successful verification a session key is generated between sensor node of network and user. User will send the encrypted queries and get access to data.

The above schemes suffer from the following problems,

1. The delayed authentication

2 Scalability is not provided at its best in terms of number of senders.

3 .Multiple senders can't broadcast at the same time.

4. Late authentication caused DoS attack.

5. Very poor performance for large scale networks.

6. Powerful senders are needed.

5. PROPOSED FUTURE WORK

The nodes of wireless sensor network are subjected to various physical attacks. The cloning attack, replay attack and man-in-middle attacks are very harmful in this case. It is easy for attacker to capture the node and copy the cryptographic information like keys and make clones of the node. Such nodes are inserted in network. The proposed work addresses such types of attacks. The proposed scheme is allowing the identification and key exchange without revealing any secret information during the conversation between the nodes. There are prover and verifier [6]. The main task of prover is to convince verifier of some secret through series of communication. The communication may have questions and challenges [6]. The only true node can correctly prove the identity. Here ID of node can also be considered. This scheme is very much secured as the attacker node will not get any of the secret information out of intercepted messages. The clustering technique like following can be used.

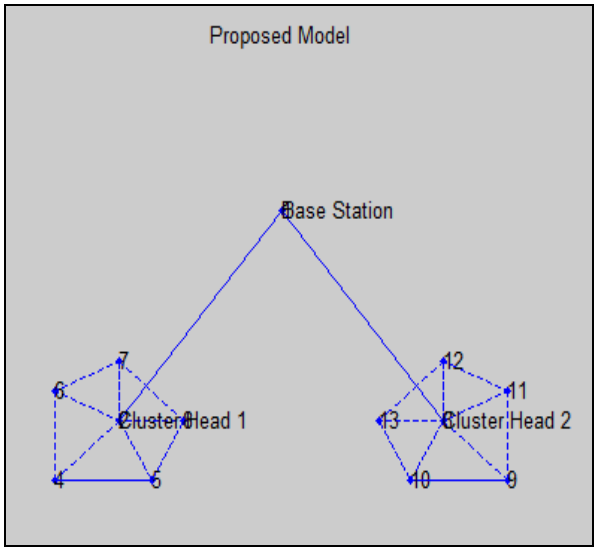

Fig.3 Clustering in Wireless sensor network.

5.1 Algorithm for Future Work

The future proposed work can be based upon following algorithm

1. Using Super imposed code find the fingerprint codeword for each node.

2. Base station will maintain N as public key which will be product of two large primes.

3. The base station generates a secret code. Prover node will try to verify to verifier. The value of secret is given to the verifier.

4. Now zero knowledge protocol is applied. Verifier will ask prover some challenge based upon its secret.

5. Prover will answer the challenge but will not open secret.

6. In this case the value of secret s is not revealed anywhere during communication and thus it will not be used by any attacker node.

6. CONCLUSION

Wireless sensor networks come with huge application domain but rather require the same level of security on other side. The paper discusses various authentication techniques available in wireless sensor network and analyzes them. Some techniques are very helpful but come with some disadvantages. The effort is also done to point out these difficulties. Authentication is one of the best security solutions which protects whole sensor network. The proposed security using authentication without opening the secret information is highly secured and will not be broken. If the zero knowledge protocol is used for repeated challenges then it will be very secured and sure scheme for the security of entire network. The computational cost of this technique also appears to be very less as there are no high calculations required. So this will reduce the energy, storage requirements of the sensor node. Thus much effort should be given to develop such highly secured authentication schemes.

7. ACKNOWLEDGEMENT

I owe a great many thanks to a great many people who helped and supported me during the writing of this paper. My deepest thanks to Prof. M .B Chandak , Head Department of CSE and the Guide of the project for guiding and correcting various documents of mine with attention and care. I express my thanks to Dr. N. V. Thakur , Co-ordinate of M.Tech for extending his support and valuable guidance. My deep sense of gratitude to Principal and all the Faculty members of my college and Library Staff for their helpful nature. I also extend my heartfelt thanks to my family and well wishers. At last I thank and request God to give me strength and power for my Progress.

8. REFERENCES

[1] Sunil Gupta, Harsh Kumar Verma"Authentication protocol for wireless sensor networks" Paper at World Academy of Science, Engineering and Technology 2010.

[2] Dan Khanh Vu "Wireless Sensor Network Architecture And Its Security Challenges" Thesis submitted at California State University, Sacramento, 2010.

[3] A. Perrig ETt Al. SPINS: Security Protocols for Sensor Networks. Wireless Networks vol. 8, 2002, Pages 521-534.

[4] Q. Huang ET Al. Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks. WSNA '03, September 19, 2003, Pages 141-150

[5] Rashmita Rautray and Itun Sarangi " A Survey on authentication Protocols for Wireless Sensor Networkss". International Journal of Engineering Science and Technology. 2011.

[6] Siba Ugata, Alefiah Mubeen and Samrat Sabat " Wireless Sensor Network security using zero knowledge Protocol. IEEE communications ICC 2011 Proceedings.

[7] Sami, S., Al-Wakeel , S., Al-Swailem, S.A., PRSA: A Path Redundancy Based Security Algorithm for Wireless Sensor Networks, IEE WNC 2007 Proceedings, 2007

[8] Rehana Yasmin, Eike Ritter " An Authentication Framework for Wireless Sensor Networks using identity based Signatures." EPSRC Project 2010.

[9] M. Tubaishat, S. Madria, (2003) "Sensor Networks : An Overview ", IEEE Potentials, April/May 2003

[10] A. D. Wood and J. A. Stankovic,(2002) "Denial of service in sensor networks",Computer, 35(10):54–62, 2002.