A Survey on Security in Wireless Sensor Networks Using Elliptical Curves Cryptography

Ms. Reena S. Satpute
M.Tech. 3rd sem (C.S.E.)
B.D.C.O.E., Sevagram
Pin Code-442001.

Prof. Amit N. Thakare
Assistant Professor
B.D.C.O.E., Sevagram
Pin Code-442001

Abstract

A wireless sensor network is deployed in the hostile environments and over large geographical regions. It is set up by a number of nodes cooperating wirelessly over the restricted frequency and bandwidth. The goal of this survey is to provide the appropriate key management between base stations to sensor node along with the detailed survey of various methodologies used to provide the security in the wireless sensor networks.

Keywords: *Elliptical curves cryptography, Key management, Secret sharing, Wireless sensor networks*

1. INTRODUCTION

Wireless sensor networks are becoming very popular now a day as they offer economically feasible and real-time monitoring solutions. While establishing the Wireless Sensor Network, the sensor nodes can be easily deployed in the unreceptive environments and thus they are broadly used in the diversity of real-time applications such as environment control, military surveillance, forest detection, harmful gas monitoring, intelligent transportations etc. Fig i) shows the architecture of WSN which provides economical solutions in a host of diverse industries such as in case of electric utilities WSNs use for remote voltage monitoring, museums use WSNs for humidity monitoring and control, health care providers use WSNs for patient monitoring and notification etc. Wireless communication is good for sensor networks as they offers the facilities as, it reduces the cost of infrastructure, allows the sensor networks to be deployed in the prohibited areas also.

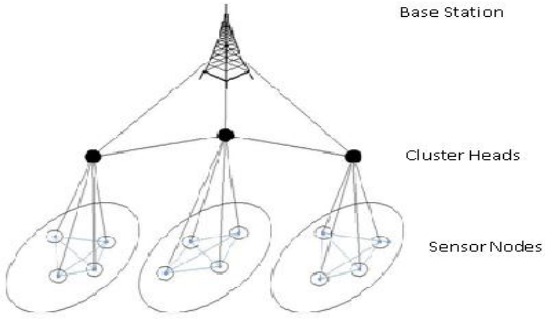

Fig. i) Wireless Sensor Network

1.1 Security Requirements

1. **Confidentiality-** Confidentiality defines the control of the message from an aggressor so that any message communicated by means of the sensor network remains confidential. In a WSN, the issue of confidentiality should attend to the following requirements: (i) Key distribution mechanism should be extremely robust (ii) A sensor node should not allow its vital information to be accessed by its neighbors (iii) Public information such as sensor identities and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks [4].

2. Integrity - Integrity defines the reliability of the data and refers to the capability to authenticate that a message has not been corrupted with, altered or changed while on the network. In a WSN, the issue of integrity should address the following requirements: only the nodes in the network should have access to the keys and only an assigned base station should have the opportunity to change the keys [4].

3. Availability - Availability defines the services of assets offered by the network, or by a single sensor node must be available whenever it is required. In a WSN, the issue of availability should address the following requirements: (i) the security mechanisms should be available all the time; a single point of failure should be avoided, (ii) the mechanism is used as a central access control

system to ensure successful delivery of every message to its recipient node [4].

4. Authentication - Authentication ensures the reliability of the message by recognizing its origin. By authenticating other nodes, cluster heads, and base stations before yielding some degree of resource, or revealing information. In a WSN, the issue of authentication should address the following requirements like, receiver node should verify that the received packets have irrefutably come from the actual sender node[4].

1.2 Connotation of Cryptography in Wireless Sensor Networks

The popularity of WSN increasing for a wide variety of applications such as climate change, environmental monitoring, traffic monitoring and home automation. To keep the WSN secure is a challenging task. Cryptography is one way to provide security. It can be provided through by symmetric key techniques, asymmetric key techniques and hash function. Since WSN are very constrained in terms of computing, communication and battery power, it requires a light weight cryptographic algorithm. Due to constraints of sensor nodes, the selection of cryptographic technique is vital in WSN.

1.3 Cryptographic Techniques

It is important to select the most appropriate cryptographic method because all the security requirements are ensured by cryptography. Cryptographic methods used in WSNs should meet the constraints of sensor nodes and be evaluated by code size, data size, processing time, and power consumption. However, sensor nodes are limited in their computational capacity and memory capabilities, so the traditional cryptographic techniques cannot be simply transferred to WSNs. Consequently, to fulfill the security requirements, either the existing techniques have to be adapted or novel techniques have to be developed. Based on the existing cryptographic techniques, we can classify them into four classes: symmetric cryptographic techniques, asymmetric cryptographic techniques and hybrid cryptographic techniques and secret sharing are discussed as follows:

1.3.1. Symmetric Cryptographic Techniques

In symmetric cryptographic techniques, a single shared key is used between the two communicating nodes both for encryption and decryption. This key has to be kept secret in the network, which can be quite hard in the exposed environment where WSNs are used. Most security schemes for WSN use only symmetric cryptography, due to its ease of implementation on limited hardware and small energy demands [7].

1.3.2. Asymmetric Cryptographic Techniques

In asymmetric cryptography, a private key can be used to decrypt and sign data while a public key can be used to encrypt and verify data. The private key need not to be disclosed while the public key can be published freely. Asymmetric cryptography is also known as Public key cryptography. Public key cryptography tends to be resource intensive, as most systems are based on large integer arithmetic. For a number of years many researchers discarded public key cryptography as infeasible in the limited hardware used in WSN. The code size, data size, processing time, and power consumption make it undesirable for public key algorithm techniques, such as the Diffie-Hellman key agreement protocol or RSA signatures, to be employed in WSNs [12]. ECC requires less energy than RSA. In 2006 Piotrowski and Peter estimated the power consumption of the most common RSA and ECC operations, such as signature generation and authentication.

Table 1: Comparison of key size between Symmetric encryption, RSA and DH and ECC

Symmetric Encryption	RSA and Diffie-Hellman	Elliptic Curves Cryptography
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

1.3.3. Hybrid Cryptographic Techniques

Symmetric and asymmetric cryptography can be applied in combination to join the advantages of both approaches. Prof. Pugliese and Santucci proposed a novel hybrid cryptographic scheme in 2008 for generation of pair wise network topology authenticated keys (TAK) in WSNs, which is based on vector algebra. Symmetric is used for ciphering and authentication, while asymmetric is used for key generation.

1.3.4. Secret Sharing scheme

Secret sharing can be used to enhance the security of the system. It is invented by Dr. Adi Shamir and Blakey in 1979. Secret sharing mainly focuses of dividing the master secret into the number of shares. Total shares will get distributed among the number of participant and for reconstructing the secret some threshold number of participants along with their secret is required. There are number of secret sharing schemes are available such as traditional secret sharing,

threshold secret sharing, threshold changeable secret sharing, verifiable secret sharing etc [12]. WSN applications can be classified into two types: monitoring and tracking. Monitoring applications includes indoor/outdoor environmental monitoring, health as well as wellness monitoring, power monitoring, inventory location monitoring, factory and process automation, and seismic and structural monitoring. Tracking applications include tracking objects, animals, humans, and vehicles too.

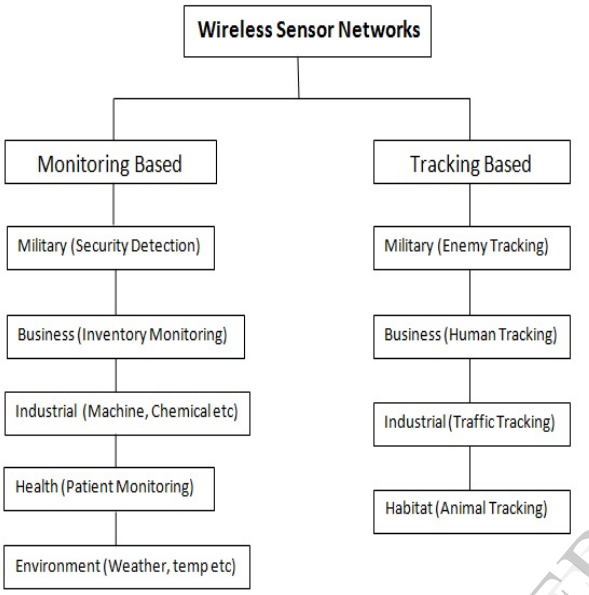

Fig. 2: Applications of WSN based on Tracking and Monitoring

Fig.2. Applications of WSN based on monitoring and tracking

2. LITERATURE REVIEW

In Wireless Sensor Network, large number of nodes that are deployed densely in close proximity to the phenomenon to be monitored. Each of these nodes gathers data and its purpose is to route this information back to a sink. Author has also concentrated on some other design issues like power consumption, fault tolerance, scalability, production cost hardware and software constraints, sensor network topology, transmission media etc[13]. Cryptography is the vital encryption method used in security implementation basically for data communications. There are two types of cryptographic methods namely asymmetric and symmetric. The drawbacks are like it requires more computation power and more memory than symmetric key cryptographic approach. Since it provides the more security it is widely used such as RSA and Elliptic Curves Cryptography algorithms [12].

In the network security and cryptography, the study of confidentiality and authenticity are very important. Confidentiality is provided by encryption as well as authenticity is guaranteed by digital signature. Traditionally, these two goals are always considered separately. Signcryption is a new paradigm in public key cryptography, which was first proposed by Zheng in 1997[11]. A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking. These sensors are connected with wireless interfaces with which they can communicate with one another to form a network. The design of a WSN depends significantly on the application, and it must consider factors such as the environment, the application's design objectives, cost, hardware, and system constraints [10]. In the Wireless sensor networks, sensor nodes cooperatively monitor the area and sense significant amounts of data which will get aggregated and then forwarded to their respective cluster head and then finally to the base stations.[9] Secure data aggregation based on secret sharing and information dispersal has proposed where sensor nodes split messages into sub shares and forward them among several disjoint paths to defend DoS attack, eavesdropping attack, and tampering attack. They have designed a secret multipath aggregation (SMA) mechanism which applies secret sharing to create shares to deal with security under the contingency of node compromise. However, these schemes are not feasible for heavy energy consumption [8]. A low-cost secret-sharing scheme for sensor network provides basic building blocks to establish secure communication through exchanging secret keys between neighbor nodes without any cryptography methods. An alternate approach extends the secret key establishment [7].

Elliptic Curve Cryptography was first projected by victor Miller and independently by Neal Koblitz in the mid-1980s and has evolved into a mature public-key cryptosystem. Compared to its traditional counterparts, ECC offers the equal level of security using much smaller keys. This result in faster computations and reserves in memory, power and bandwidth those are especially important in constrained environments. More significantly, the advantage of ECC over its competitor's increases, as the security needs increase in excess of time. ECC operates over a group of points on an elliptic curve defined over a finite field [6].The concept of

intra-cluster key sharing i.e. how to establish pair wise key between sensor nodes and their respective cluster heads has been proposed. Intra-cluster key sharing is somewhat more challenging as compare to the inter-cluster key sharing. Intra-cluster key sharing has proposed by author to overcome the most challenging problem of security in the wireless sensor networks. It improves the overall efficiency in saving the storage overheads and communication overheads [5]. An identity based key agreement protocol based on the technique of elliptic curve cryptography (ECC) between users of different networks with independent private key generations (PKGs). Elliptic curves are used to obtain more computational efficiency[3].They have used protocol for situations that two users of independent organizations or networks with separate servers want to share a secret key via an insecure link. In public key cryptosystems, each user has a private key and a corresponding public key [4]. Wireless sensor networks (WSNs) are subjected to various attacks because of the vulnerable environment, limited recourse, and open communication channel. To protect WSN they have presented a Secret sharing-based key management. It utilizes the advantages of hierarchical architecture and adopts two-level key management and authentication mechanism, which can efficiently protect the all over network communication security and survivability [2].

In the secret sharing scheme, it distributes the keys based on secret sharing mechanism by the clustered architecture, which not only localizes the key things but also keeps scalability. The Secret sharing-based key management provides various session keys, the network key for base station (BS) and cluster heads (CHs); the cluster key between the cluster head and member nodes [2].User authentication in wireless sensor networks (WSNs) is a critical security issue due to their unattended and hostile deployment in the field. Since sensor nodes are equipped with limited computing power, storage, and communication modules, authenticating remote users in such resource-constrained environments is a paramount security concern. To overcome the weaknesses, they have proposed a new authentication protocol for wireless sensor networks using elliptic curves cryptography [1].

3. COMPARISION

Year	Title of paper	Algorithm Used	Applications
2002	The survey of sensor networks	Basic information about WSN and their design issues	Museums
2005	The efficient security mechanisms for large-scale distributed sensor network	Asymmetric and symmetric key cryptography	Fire alarm Control system
2005	A signcryption scheme based on elliptic curve cryptosystem	Digital signature with public key encryption	Military surveillance
2008	The survey of security architecture in sensor networks	Overall survey of various security techniques used in sensor networks	Harmful gas monitoring
2009	Secure data aggregation based on secret sharing and information dispersal	Secret sharing and information dispersal secret multipath aggregation (SMA)	Intelligent transportati-ons

2010	A low-cost secret-sharing scheme for sensor network	Secret keys establishment and exchanging between neighbour nodes	Environm-ent control
2011	A Secured Authenticatio n Protocol for WSN using ECC	Scalar multiplicatio n is performed through a combination of point-additions	Intelligent Transport-tations
2012	Intra-cluster key sharing in sensor networks	Intra-cluster key sharing by establishing pairwise key between sensor nodes and cluster head	Healthcare
2012	An identity based key agreement protocol based on elliptic curve cryptography (ECC)	Public key generation along with signed with their private key.	Intelligent Transport-tations
2013	Secret sharing-based key management in Wireless sensor networks	Secret sharing-based key management with session key and cluster key generation	Military Surveillance
2013	User authentication in wireless sensor networks (WSNs) based on elliptic curve cryptography (ECC)	Authenticati on protocol for wireless sensor networks using elliptic curves cryptograph y	Military Surveillance

4. CONCLUSION

As wireless networks are hostile, they are highly affected with the noise and interference. Thus to maintain the security among the data being aggregated from various nodes are very important. In this survey the various techniques to maintain the security to the data in WSN has been studied.

The proposed methodology to provide security to the data will be the two-way key management between base station to cluster heads and from cluster heads to the sensor nodes by using ECC along with the concept of secret sharing scheme which will not only to avoid the single user authority but improves the security to the data.

5. REFERENCES

[1] Wenbo Shi and Peng Gong, "A New User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography" in proceedings of *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks*,vol-730831, 1-7 , 2013.

[2] Yiying Zhang,Chunying Wu,"A secret sharing based key management in hierarchical wireless sensor" proceedings in *International journal of Distributed sensor network*, vol. no 5, pp.1-7, 2013.

[3] Mohammad Sabzinejad Farash,"An ID-Based Key Agreement Protocol Based on ECC Among Users of Separate Networks" in proceedings *of 9th International ISC Conference on Information Security and cryptology*, p.no.31-37 , 2012

[4]Weiming Shen,"Security and Privacy Considerations for Wireless Sensor Networks in Smart Home Environments", in proceedings of *the IEEE 16thInternational Conference on Computer Supported Cooperative Work in Design*, vol no. 978 page no. 626-630, 2012

[5] Eleni Klaoudatou,"A Survey on Cluster-Based Group Key Agreement Protocols for WSNs" in

proceedings of IEEE Communications Surveys &Tutorials, Vol. 13,pp-33, Third Quarter 2011

[6] M. Bertier and G. Tredan, "Low cost secret sharing in wireless sensor networks" in proceedings of *IEEE Communication Magazine*, pp.65-67, 2010

[7] T.Claveirole,"Secured wireless sensor against aggregator comprimise" in proceedings of *IEEE Trans.on Sensor network*, vol.3pp.28–38,Aug. 2009

[8] Jennifer Yick, Biswanath, "Wireless sensor network survey",in Proceedings of the *Elsevier of computer networks* vol. 4, page no. 52-68, 2008

[9] M. Luk,"MiniSec:A secure sensor networks communication architecture" in proceedings of the *1st IEEE International Workshop on Sensor Network Protocols and Applications*,2007

[10]Peng Changgen, Li Xiang, "Threshold Signcryption Scheme Based on Elliptic Curve Cryptosystem and Verifiable Secret Sharing" in proceedings of *IEEE conference on sensor networks*, page no.1136-1139, 2005

[11] S. Zhu, "The efficient security mechanisms for large-scale distributed sensor network" in *proceedings IEEE Trans.on Sensor network*, pp.528–538, Aug. 2005

[12]Adi Shamir, "How to share a secret", *proceedings in Communications of the* ACM, v.22 n.11, p.612-613, 1979.

[13]I.F.Akyildiz, "A Survey on sensor networks" in the proceedings of *the Elsevier,* Feb 2002

[14] Gaurav Sharma,"Security Frameworks for Wireless Sensor Networks-Review" in 2nd International Conference on Communication, Computing & Security, Elsevier , page no. 978 – 987, 2012