International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 5, Issue 5, September - October 2016 **ISSN 2278-6856**

Wireless Sensor Networks Security Survey Using Cryptography

[1]KRISHNACHAITANYA.KATKAM , [2]KAMULU DEEPTHI

[1]Asst Prof (CSE) Kshatriya College Of Engineering Armoor

[2]Student Kshatriya College Of Engineering Armoor

Abstract

In the threatening situations and over expansive geological areas a wireless sensor network is sent. Over the ambient recurrence and transfer speed it is set up by various different hubs coordinating remotely. To give the fitting key administration between base stations to sensor hub alongside is the main objective of this study to give the security in the remote sensor systems the point by point review of different procedures is used.

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

1.INTRODUCTION

Economically feasible and real-time monitoring solutions are offered by Wireless sensor networks hence they are becoming very popular now a day. The sensor nodes can be easily deployed in the unreceptive environments while establishing the Wireless Sensor Network 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.

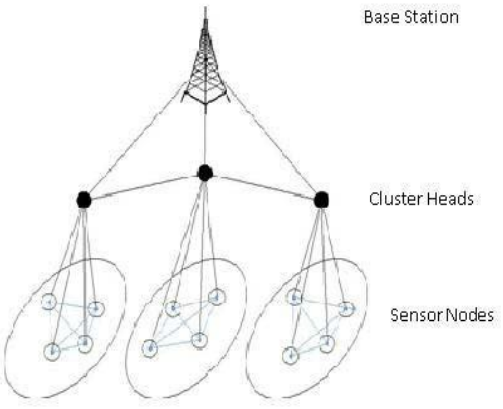

Fig i. Wireless Sensor Network

Fig i) shows the architecture of WSN which provides economical solutions in a host of diverse industries such as in case of electric utilities control system to ensure 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. They offers the facilities as, it reduces the cost of infrastructure, allows the sensor networks to be deployed in the prohibited areas also with the help of wireless communication.

Availability – Availability defines the services of assets offered by the network, or by a single sensor node must be available whenever it is required. The issue of availability in a WSN, should address the following requirements:

(i) all the time the security mechanisms should be available; 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 .

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

Connotation of Cryptography in Wireless Sensor Networks: For a wide variety of applications such as climate change, environmental monitoring, traffic monitoring and home automation the popularity of WSN is increasing. Securing the WSN is a challenging task. One way to provide security is Cryptography. Symmetric key techniques, asymmetric key techniques and hash function are used to provide security. It requires a light weight cryptographic algorithm, since WSN are very constrained in terms of computing, communication and battery power. The selection of cryptographic technique is vital in WSN due to constraints of sensor nodes.

Security Requirements: Confidentiality- Confidentiality defines the control of the message from an aggressor so that any message communicated by means of the sensor

network remains confidential. The issue of confidentiality in a WSN, should attend to the following requirements:

(i) Mechanism of key distribution should be extremely robust
(ii) A sensor node should not allow its vital information to be accessed by its neighbours
(iii) To protect against traffic analysis attacks in certain cases public information such as sensor identities and public keys of the nodes should also be encrypted.

Integrity - To authenticate that a message has not been corrupted with, altered or changed on the network is defined by integrity as the reliability of the data and refers to the capability. In a WSN, the issue of integrity should address the following requirements:

--In the network only the nodes should have access to the keys and only an assigned base station should have the opportunity to change the keys.

Cryptographic Techniques:

To select the most appropriate cryptographic method is important because cryptography ensures all the security requirements. To meet the constraints of sensor nodes Cryptographic methods are used in WSNs should be evaluated by code size, data size, processing time, and power consumption. The computational capacity and memory capabilities of sensor nodes are limited, 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. We can classify them into four classes based on the existing cryptographic techniques: symmetric cryptographic secret is required. There are number of secret sharing schemes techniques, asymmetric cryptographic are available such as traditional secret sharing, techniques and hybrid cryptographic techniques and secret sharing are discussed as follows: 1.

Symmetric Cryptographic Techniques: In symmetric cryptographic techniques for both encryption and decryption, a single shared key is used between the two communicating nodes. It is quite hard to keep the key secret in a network 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.

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

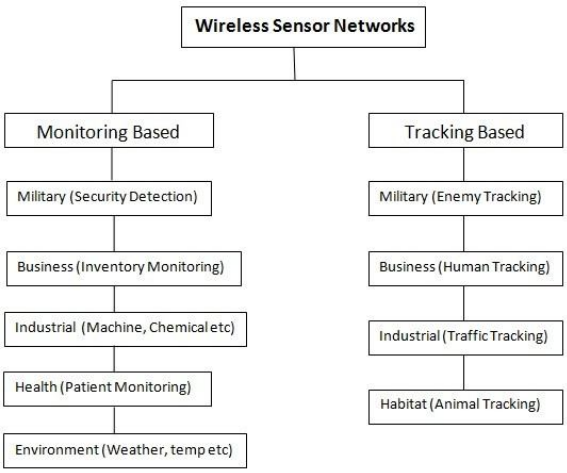

Fig 2.Applications of WSN based on Monitoring & tracking

2.LITERATURE REVIEW

A large number of nodes that are deployed densely in close proximity to the phenomenon to be monitored in Wireless Sensor Network. Data is gathered by each of these nodes and its purpose is to route this information back to a sink. Power consumption, fault tolerance, scalability, production cost hardware and software constraints, sensor network topology, transmission media etc are some of the design issues concentrated . In security implementation cryptography is the vital encryption method, basically used for data communications. Asymmetric and symmetric are the two cryptographic methods.

It requires more computation power and more memory than symmetric key cryptographic approach so, they are the drawbacks. More security is provided by it so, it widely uses RSA and Elliptic Curves Cryptography algorithms. The study of confidentiality and authenticity are very important in the network security and cryptography.

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

Secret sharing scheme: To enhance the security of the system secret sharing can be used. Dr. Adi Shamir and Blakey invented it in 1979. Dividing the master secret into the number of shares is focused by secret sharing. Total shares will get distributed among the number of participant and for reconstructing the secret some threshold number of participants along with their confidentiality is provided by encryption as well as authenticity is guaranteed by digital signature. Traditionally, these two goals are considered separately always.In 1997, Zheng proposed Signcryption, which is a new paradigm in public key cryptography. The remote environmental monitoring and target tracking are the important applications of a Wireless Sensor Network (WSN). To form a network, these sensors are connected with wireless interfaces with which they can communicate with one another.

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]. Sensor nodes cooperatively monitor the area and sense significant amounts of data in the Wireless sensor networks, which will get aggregated and then forwarded to their respective cluster head and then finally to the base stations.

Based on secret sharing and information dispersal secure data aggregation 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. A secret multipath aggregation (SMA) mechanism has been designed by them which applies secret sharing to create shares to deal with security under the contingency of node compromise. For heavy energy consumption these schemes are not feasible . A low- cost secret-sharing scheme for sensor network provides basic building blocks to establish secure communication through exchanging secret keys between neighbour nodes without any cryptography methods.

An alternate approach extends the secret key establishment .Victor Miller first projected Elliptic Curve Cryptography Neal

Koblitz and independently projected it in the mid-1980s and has evolved into a mature public-key cryptosystem. ECC offers the equal level of security using much smaller keys compared to its traditional counterparts. This result in faster computations and reserves in memory, power and bandwidth those are especially important in constrained environments. The advantage of ECC over its competitor's increases more significantly, 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.

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. Overall efficiency in saving the storage overheads and communication overheads is improved by it. 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). More computational efficiency is obtained by using elliptic curves .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, Each user has a private key and a corresponding public key in public key cryptosystems . Various attacks are subjected by wireless sensor networks (WSNs) 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 overall network communication security and survivability .

It distributes the keys in the secret sharing scheme, 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 . In wireless sensor networks (WSNs) user authentication 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. A new authentication protocol have been proposed by them to overcome the weaknesses, for wireless sensor networks using elliptic curves cryptography .

3.CONCLUSION

They are highly affected with the noise and interference as wireless networks are hostile. Thus to maintain the security among the data being aggregated from various nodes are very important. To maintain the security to the data in WSN various techniques has been studied in this survey. The survey is 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.

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]

[2]. 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

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

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

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

Author

KRISHNACHAITANYA.KATKAM completed MTech CSE from JNTU Hyderabad Having 9+years of experience in Teaching. At Present Working as a Asst Prof in Kshatriya College Of engineering Chepur,Armoor. Interested in mobile computing,computer forensics, computer networks.

Deepthi Kamulu Pursuing B.Tech final year in Computer Science & Engineering at KCEA, Armoor.