International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 9 5608 - 5613

Different Security Mechanisms for Wireless Sensor Networks

Nidhi Chhajed
Research Scholar, CSE Department
Sanghvi Institute of Management and Science,
Indore (M.P), India
nidhichhajed31@gmail.com

Mayank Kumar Sharma
Assistant Professor, CSE Department
Sanghvi Institute of Management and Science,
Indore (M.P), India
mayank.sharma@sims-indore.com

***Abstract*—** In today's world security becomes one of the important constraints in every research field. As increasing use of Wireless Sensor Networks (WSN) in various crucial applications security of wireless networks is becoming more important day by day. Today almost each and every important area makes use of wireless sensor networks. As Wireless Sensor Network is infrastructure-less network; data moves openly from one node to another thus it can be captured easily by attackers. To avoid data from being stolen security mechanism has to be applied. Many protocols are available for providing security on wireless network. We perform a detailed study of different security mechanisms used in sensor network against some criteria such as nature of algorithm, working, its benefits and some of the disadvantages of mechanism and also compare them.

Keywords- Wireless sensor network (WSN), security mechanisms, Key management protocols, RSA, cryptography.

*****

I. INTRODUCTION

Wireless Sensor Networks[1] has become one of the most important research fields for researchers due to its applications in various areas. There are many significant applications where it can be deployed like military[2], surveillance, areas suffering from natural disasters etc. Wireless Sensor Network is a type of ad hoc network where numbers of sensor nodes are connected wirelessly to communicate with each other and carry information through electromagnetic waves. These nodes are called motes. Motes have the capability of receiving and sending information to each other. Wireless Sensor Network has characteristics like flexibility of network, low cost and its small size. Though these sensors do not require any infrastructure for deployment, they can be deployed easily in the area where it is hard to establish wired network.

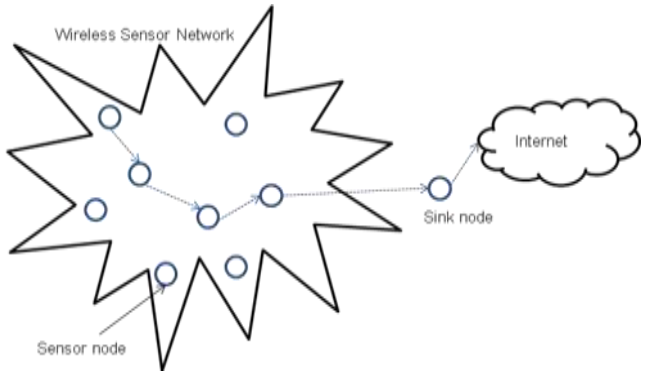

Figure 1: Wireless Sensor Network

Some applications like military requires highly secure network as information is very crucial and has to be saved from the outsiders, so security[3] is main concern. Its exploitation in various areas raise requirement of security so that information travelling between these nodes can be received only to the intended receiver and cannot be leaked. There are various types of security threats that exist in Wireless Sensor Network. These include black hole attack, wormhole attack, Sybil attack, denial of service attack[4] and many more which can harm the network if proper action is not taken. To provide security in Wireless Sensor Network various security mechanisms are provided so that nodes cannot be compromised and data transmits securely. There are many types of security mechanisms used among which some uses different types of key management techniques. In this paper, miscellaneous security mechanisms are discussed for achieving secure and unbiased network. Section 2 describes different security mechanisms for Wireless Sensor Network; Section 3 contains comparison among different mechanisms and Section 4 concludes the paper.

II. LITERATURE REVIEW

RSA[5] cryptosystem is one of the well-known security cryptographic algorithms, which is a collection of three phases- key generation, encryption process and decryption process.

Let's reflect on the procedure how keys are generated in RSA cryptosystem-

A. *Key Generation*

(1) Select p and q both prime number, p is not equal to q.
(2) Calculate n = p x q.
(3) Calculate ø (n) = (p -1) x (q-1).
(4) Select integer e whose gcd (Ø (n), e) = 1; 1 < e <Ø (n).
(5) Calculate private key d = e^{-1} (mod Ø (n)).
(6) Public key PU = {e, n}.
(7) Private Key PR = {d, n}.

B. *Encryption Procedure*

Plaintext- Message (M)

Cipher text- $C = M^e \bmod n$.

C. *Decryption Procedure*

Cipher text- C

Plaintext- $M = C^d \bmod n$.

Where, M is message, p and q are prime numbers, N is common modulus, e and d are public and private keys.

RSA technique ensures that information is secret and genuine, thus it provides secure communication over the system. Its security is based on the complexity in factoring very large numbers. Based on this principle, the RSA encryption uses prime factorization as the trapdoor for encryption. It uses public key encryption in which anybody use public key to encrypt the data and hurl over the network. It provides authentication and security over the network in order to provide private key to decrypt the information as a result only indented receiver can decrypt the information. RSA algorithm is used for both data encryption and digital signature. The curb of using public key cryptography for encryption and decryption is speed. Its computation takes time to calculate the arithmetical operation of RSA algorithm. Public key used for encryption must be authenticated. If hacker knows the factors of a large prime number, then this breaks the security of algorithm, since the values of public key and private keys are known with the help of factors. Thrashing of private key might leak the information in the communication network. RSA algorithm refers to an asymmetric cryptography in which two dissimilar keys are used for encryption and decryption, consequently its computational cost is high as contrast to symmetric cryptography. There are various attacks in RSA cryptosystem such as factorization problem, low decryption exponent, common modulus, short message, cyclic attack etc.

The Diffie-Hellman Key Exchange

The Diffie-Hellman Key Exchange is one of the most accepted and appealing methods of key circulation. It is a public-key cryptographic system whose singular principle is to distribute keys. Diffie-Hellman is an example of a Public-Key Distribution Scheme (PKDS) whereby it is used to replace a solo piece of information, and where the value acquired is usually used as a session key for a private-key plot.

How Diffie-Hellman Works?

The Diffie-Hellman distribution system works as follows:

Assuming two people, named Alice and Bob correspondingly, wish to exchange a key over an insecure communication channel:

1. Both Alice and Bob agree on the selection of a large prime number n, a primitive element g, and the one-way function f(x) = g% mod n (Note: both n and g are made public).

2. Alice selects a large random integer a and sends Bob the value A = g& mod n. Bob selects a large random integer b and sends Alice the value B = g' mod n.

3. Alice computes s = B& mod n (= g*+ mod n). Similarly, Bob computes s = A' mod n (= g+* mod n).

4. Alice and Bob now both share the same secret key s. The computation of x = f(¹(y) is extremely hard; therefore, someone attempting to listen to the key-exchange cannot determine s even by knowing the values of A, B, n, and g.

The major disadvantage of Diffie Hellman Key Exchange algorithm is that it is easily vulnerable to man-in-the-middle attacks. A third party C, can swap keys with both A and B, and can take note to the communication between A and B. The algorithm is computationally rigorous. Each multiplication varies as the square of n, which have to be extremely large. The number of multiplications requisite by the exponentiation increases with growing values of the exponent, x or y in this case.

Mi Wen[6] et al. proposed a unified security framework with 3 key management protocols – MPKM, MGKM, and TKM. They perform evaluation on the basis of scalability, key connectivity and compromise resilience and also perform comparison to current keying protocols for Wireless Sensor Network and WMN. A wireless mesh network (WMN) is a communications network of radio nodes ordered in a mesh topology. It is also a form of wireless ad hoc network. Wireless mesh networks frequently consist of mesh clients, gateway routers and mesh routers. The mesh clients are often cell phones, laptops and additional wireless devices even as the mesh routers advance traffic to and from the gateways which might, but require not, join to the Internet. The exposure area of the radio nodes operate as a single system is every so often called a mesh cloud.

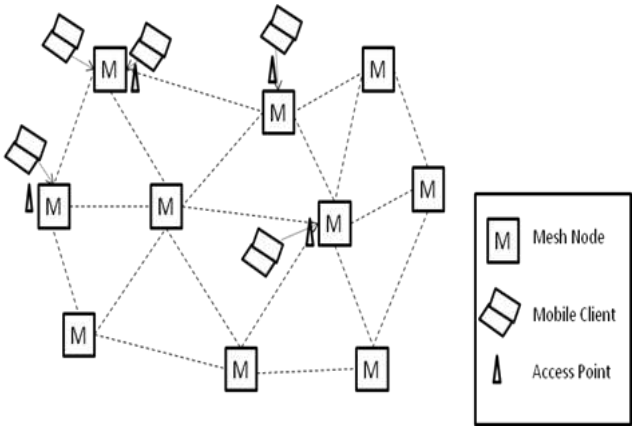

Figure 2: A community deployed WMS[6]

There were many security protocols differ on the basis of complexity, scalability and network abstraction level. The sensor networks can be mainly classified into two types: pair

wise key management protocols plus set key organization protocols. In pair wise key management protocols [7-12], every two of a kind of communication systems must establish a common key. One striking idea in the pair wise key management is key pre-distribution, meaning pre-installing a restricted number of secrets in sensor nodes past to actual consumption; after the deployment, if two adjacent nodes have a few common keys, they can group or set a safe and sound link by the shared keys, whereas in the group key supervision protocols [13-15], the key in idea is to broadcast information which is constructive only for trusted and reliable nodes. Collected with its pre-distributed secrets, this transmitted information enables a trusted sensor node to rebuild a faction key. Nearly all pair wise key and group key organization protocols in WSNs are based on symmetric key cryptography, like Du's key Matrix based, Camtepe's Combinatorial blueprint based, Liu's polynomial based protocols. Most pair wise key and group key management protocols in WSNs are based on symmetric key cryptography. [16]The right collection of algorithms and connected parameters along with code optimization can make public key cryptography practicable for sensor networks. This paper proposed 3 different types of key management scheme to provide security in Wireless Sensor Network and WMSNs. Although the framework is quite simple but effective solution for achieving security and do not provide high level of security. In future, it can be enhanced to achieve perfect security and robustness for integrated network.

Cai-Xia Zhang[17] et al. described the source limitations and vulnerabilities of the sensor nodes of Wireless Sensor Networks, we offer the novel kind of lively key protocol for wireless sensor network, using the unidirectional property of hash function and the philosophy of Hill to learn the dynamic key matrix. The results show that this protocol cuts off storage space and communication energy expenditure also. The low power, low storage capacity, and high-security type of security management mechanism for the normal operation of wireless sensor networks is very important. Key management is the input issue in the safety of WSN. The current key management scheme is divided into symmetric key and asymmetric key management system. Because of the difficulty of algorithm, the asymmetric key can't be openly applied to the resource-constrained WSN's. Symmetric key organization system can normally be divided into the next three categories: methods based on key allocation centers, pre-distribution and packet-based clustering approach. This paper proposes a key management based on dynamic key matrix for wireless sensor networks to reduce the amount of key storage nodes and improve connectivity and confrontation to attack of the net. In this paper, the dynamic key agreement can be divided into three stages: the stage of presetting initial information, the stage of establishing link key, and the stage of updating link key.

i. *Unidirectional One-Way Hash Function*

In the understanding of this method, it needs to express the dynamic generation of key matrix information, while ensure that even if the plaintext information is attained, the key matrix can't be speedily derived below the information. This can be achieved by using the one-way hash function. There are two common modes of communication in Wireless sensor networks, which are communication between adjacent nodes and communication between nodes and base stations. Key establishment protocol proposed in this paper is based on this assumption on the network deployment phrase. This paper focuses on the link's establishment process under the single-hop key. This paper provides a new dynamic key management protocol which uses a password matrix for encryption and decryption. As different keys are used it prevents packets from being captured and enhances security. It also reduces transmission of session keys between nodes and save energy consumption.

Benamar Kardi[18] et al. proposes a trivial implementation of public key infrastructure called cluster based public infrastructure (CBPKI), CBPKI is based on the safety and the validity of the base station for executing a set of handshakes anticipated to start session keys amid the base station and sensors over the network used for ensuring data privacy and reliability.

Hierarchical Network Architecture

Due to the difficulty of supervision a flat network caused by the growing figure of sensors as well as the number of rumour sent to the base station, the hierarchical structural design tries to make simpler the management of the network by combining sensors into groups called clusters. One of the members of the cluster is elected as cluster head responsible of additional tasks such as cluster management, the rest of sensors are called cluster members.

Hierarchical architecture for supervision security or routing seems to be more capable since the cluster head is proposed to play the key role for security or routing which minimizes the figure of operations for executing the basic operations for routing or security protocol since a division of operations is delegated to the cluster skull.

Wireless Sensor Networks was treated with a great deliberation to the partial possessions of sensors such as energy, computing and storage capacities. This has given birth to a variety of scheme based essentially on symmetric cryptography which makes them vulnerable against several attacks. In this section we give an overview of the most known security schemes:

Shared key

It uses a single shared key to encrypt traffic over the network. As any other scheme based on single shared key, this

scheme is vulnerable against capture attack which is more possible in sensor network, since the capture of only one sensor can compromise the shared key and then the whole network [19].

Secure pebblenets

This solution proposed by Basagni [20] is an extended version 0 of the shared key solution. By using a set of symmetric keys preloaded to each sensor over the network, which is divided into cluster in order to simplify the management of security.

Simplified SSL handshake

In [21], the authors give the energy cost analysis of a simplified version of SSL applied to WSN, which reduces the amount of exchanged data between any pair of nodes to save energy and band-width. Compared to the original SSL protocol this proposition is more energy saving how- ever it is not energy efficient, since a handshake between each pair of sensors consumes lot of sensor resources.

CBPKI uses two types of cryptography, Symmetric and asymmetric algorithms with an optional use of a hash function as a MAC (message authentication code). We propose to use the ECC (Elliptic Curve Cryptography) for data encryption considered to be more efficient regarding energy consumption. A public key cryptography based security scheme is presented in this paper.

According to Pengcheng Zha[22] et al. the weak spot of session key construction based on node's individual location, we put forward a hybrid key administration proposal which based on clustered WSNs. The use of hierarchical thinking, dipping the amount of key storage space and computing, while following network topology, lively key management for which aims to put off leakage. Through analyzing, it shows that the plan contain certain advantages in key connectivity, communication, security and energy consumption.

Large-scale WSNs usually use the hierarchical structure, and making the system divided into clusters. Each cluster has a cluster head and multiple cluster members; the lower cluster is the member of high level, and making the top cluster head nodes communicating with the base station.

Basic idea is that the cluster head in clustered wireless sensor network has a higher aptitude of information processing and storage capacity than normal nodes, which is responsible for node clustering. Cluster members produce their individual key and nearby key pair based on the in order of their geographic site and preloaded master key. After key production, the master key repeatedly separated from memory. On the one hand, the regular members of the cluster doesn't identify the front announcement session key, it can't access to the message information of the front-end clusters while the front-end using joint function to create tree structure session key, from doing this cluster head can have a relatively small amount of storage. On the other hand, common nodes in the completion of loading master keys to produce the key pair will be robotically deleted, in order to avoid a cluster node captured the whole security compromised.

3 Phases:

i. *Key Pre-Distribution Phase*

All nodes contain main key K_m and node ID which is generated randomly before deployment. Every cluster head also have session key PK(r) and a private key, where PK(r) = $K_{m.}$

ii. *Key Establishment Phase*

Key establishment is divided into two types: One is to construct a key tree amid cluster head and base station, the other one is to set up communication key connecting members of the same cluster.

iii. *Key Maintenance Phase*

Whenever a node got compromised, added to the network or removed from the network then this type of condition is handled by this phase.

The above key management technique is used in favor of clustered WSN which creates an exclusive session key between cluster heads. This technique is simple to uphold and more defiant against attacks. Future work will be to discover compromised nodes by means of trust model.

III. COMPARISION OF EXISTING ALGORITHM WITH PROPOSED ALGORITHM

S. No.	Algorithm	Type of Algorithm	Advantages and Drawbacks
1.	RSA	Asymmetric cryptography	▪ Use different keys for encryption and decryption. ▪ Consume more resources as two keys are used. ▪ Most widely used ▪ Suffer from attacks like factorization.
2.	Diffie Hellman	Key exchange algorithm	▪ Public key algorithm. ▪ Used only for exchanging key in the network. ▪ It cannot be used in digital certificates.
3.	Matrix based Pairwise Key Management (MPKM) Protocol	Symmetric cryptography	▪ Pairwise key establishment. ▪ Key updation is done by modifying symmetric matrix construction. ▪ Information is send by individual nodes.
4.	Matrix based Group Key	Symmetric cryptography	▪ Work for group key, scalable, light weight.

	Management (MGKM) Protocol		▪ Nodes send information individually.
5.	Threshold based Key Management (TKM) Protocol	Asymmetric cryptography	▪ Key sharing used in Wireless Mesh Network, scalable, lightweight. ▪ Cluster Head (CH) is used to collect information and merge from nodes. ▪ Less adjustment in the existing network can be done to adopt the technology.
6.	Hybrid Key Management Scheme	Based on clustered wireless sensor network	▪ It can be used only for clustered sensor network. ▪ Reduce amount of key storage ▪ Cluster head (CH) manage keys that is key allocation and distribution is done by CH ▪ If cluster head is captured then whole network will be compromised.
7.	Dynamic Key Protocol	Symmetric Key management	▪ Based on password matrix. ▪ It uses combination of hill cipher algorithm and unidirectional hash function for creating key matrix. ▪ Reduces energy consumption and storage space.
8.	Public Key Infrastructure (PKI)	Public key cryptography	▪ Most powerful and most efficient security mechanism. ▪ It fulfils all security aspect such as confidentiality, integrity, authenticity etc.
9.	Cluster based Public Key Infrastructure	Public key cryptography	▪ It is based on security and authenticity. ▪ It uses set of handshakes to establish session key between bas station and motes for ensuring data integrity and confidentiality.
10.	Secure Pebblenets	Symmetric key cryptography	▪ I is enhancement of shared key cryptography ▪ It uses set of symmetric key instead of using a single key for sharing information. ▪ Both inter cluster nodes and intra cluster nodes use different set of keys. ▪ Data confidentiality and integrity is achieved by this technique.

Table 1- Comparison of different security mechanisms

IV. CONCLUSION

In this paper, study of different security mechanisms is done on various parameters. Above table gives a brief description of different security techniques.

A. In WSN, security is one of the biggest issues for preventing data to be discovered by unknown source.

B. There are many security mechanisms among which some provide data integrity, confidentiality and many other issues related to security.

C. Some uses symmetric key management, some uses asymmetric key management, some mechanism can be applied to single node while some can be apply only for clustered network.

To prevent data from being leaked future work will design a new security mechanism which will be more secure than existing once and which can transmit data securely.

REFERENCES

[1] Pooja, Manisha and Dr. Yudhvir Singh, "Security Issues and Sybil Atack in Wireless Sensor Networks", International Journal of P2P Network Trends Technology, Volume3 Issue1 (2013), p.p. 7-13.

[2] Evaluation of AODV and DSR Routing Protocols of Wireless Sensor Networks for Monitoring Applications: Asar Ali, Zeeshan Akbar, Master's Degree Thesis- (October 2009).

[3] Kalpana Sharma and M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats" IJCA "Mobile Ad-hoc networks" MANETs (2010), pp-42-45.

[4] Nidhi Chhajed and Mayank Sharma, " Detection and Prevention Techniques for Black hole Attack in Wireless Sensor Networks (WSN's): A Review," International Journal of Advanced Research in Computer Science and Software Engineering, November 2014, vol 4 Issue 11, pp. 326-329.

[5] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Vol. 21, pp.120-126, 1978.

[6] Mi Wen, Zhi Yin and Yu Long, "An Adaptive Key Management Framework for the Wireless Mesh and Sensor Networks," Scientific Research, September 2010, pp. 689-697.
doi: 10.4236/wsn.2010.29083
http://www.SciRP.org/journal/wsn

[7] S. A. Camtepe and B. Yene, "Key Distribution Mechanism for Wireless Sensor Networks," TR-05-07 Rensselaer Polytechnic Institute, Computer Science Department, March 2005.

[8] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," *Proceeding of the 9th ACM Conference on Computer and Communication Security*, Washington, DC, 2002, pp. 41-47.

[9] H. Chan, A. Perrig and D. Song, "Random Key Pre-distribution Schemes for Sensor Networks," *IEEE Symposiumon Security and Privacy*, 2003, pp, 197-213.

[10] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz and A. Khalili, "A Pairwise Key Predistribution Scheme for Wireless Sensor Networks," *ACM Transactions on Information and System Security*, Vol. 8, No. 1, 2005, pp. 228-258.

[11] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," *ACM Transactions on Information and System Security*, Vol. 8, No. 1, 2005, pp. 41-77.

[12] M. Wen, K. F. Chen, Y. F. Zheng and H. Li, "A Reliable Pairwise Key-Updating Scheme for Sensor Networks," *Journal of Software*, Vol. 18, No. 5, 2007, pp. 1232-1245.

[13] D. Liu, P. Ning and K. Sun, "Efficient Self-Healing Group Key Distribution with Revocation Capability," *Proceedings of the 10th ACM Conference on Computer and Communications Security*, Washington, DC, 2003, pp. 231-240.

[14] W. Zhang and G. Cao, "Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-Based Approach," *Proceedings from the Conference of the IEEE Communications Society*, 2005, pp. 503-514.

[15] M. Wen, J. S. Lei, Z. Tang, X. X. Tian, K. F. Chen and W.D. Qiu, "A Verified Group Key Agreement Protocol for Resource-Constrained Sensor Networks," *Lecture Notes in Computer Science*, Vol. 5854, 2009, pp. 413-425.

[16] G. Gaubatz, JP. Kaps and B. Sunar, "Public Key Cryptography in Sensor Networks Revisited," *Proceedings of the 1st European Workshop on Security in Ad-Hoc and Sensor Networks*, Springer, 2004, pp. 2-18.

[17] Cai-Xia Zhang, Liang-Lun Cheng, Xiang-Dong Wang, "New Kind of Dynamic Key Protocol for Wireless Sensor Network," Scientific Research, June 2011, pp. 183-188 doi: 10.4236/wsn.2011.36021 http://www.SciRP.org/journal/wsn

[18] Benamar Kardi, Dijilali Moussaoui, Mohammed Feham, Abdellah Mhammed, "An Efficient Key Management Scheme for Hierarchical Wireless Sensor Network," Scientific Research, June 2012, pp. 155-161. http://dx.doi.org/10.4236/wsn.2012.46022

[19] S. Rafaeli and D. Hutchison, "A Survey of Key Management for Secure Group Communication,'' ACM *Computing Survey*, Vol. 35, No. 3, 2003, pp. 309-329.

[20] S. Basagni, K. Herrin, et al., "Secure Pebblenets," Proceedings of the 2nd *ACM International Symposium on Mobile ad hoc Networking & Computing*, Long Beach, 4-5 October 2001, pp. 156-163.

[21] A. S. Wander, N. Gura, H. Eberle, V. Gupta and S. C. Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks," *Proceedings of* 3*rd IEEE International Conference on Pervasive Computing and Communications*, Kauai Island, 8-12 March 2005, pp. 324-328.

[22] Pengcheng Zhao, Yong Xu, Min Nan, "Hybrid Key Management Scheme Based on Clustered Wireless Sensor Networks," Scientific Research, August 2012, pp. 197-201. http://dx.doi.org/10.4236/wsn.2012.4802