Survey on Security Improvement using Wireless Sensor Networks

R. Santhosh, PhD
Assistant Professor
Department of Computer Science and Engineering
Faculty of Engineering,
Karpagam University,
Coimbatore,Tamil Nadu

M. Shalini
PG Scholar
Department of Computer Science and Engineering
Karpagam University,
Coimbatore, Tamil Nadu

ABSTRACT
Depending on applications used in WSN, Security is one of the greatest challenge in WSNs. To ensure confidentiality of data in sensor networks, various types of security mechanisms are proposed. Drawbacks like security vulnerabilities are associated with those schemes. In this paper a survey is taken related to the security purpose. Implementation of security for wsn influence a great deal due to their size and energy limitations.To rectify these drawbacks chaotic maps and genetic operations are used. This algorithm is helps in encoding the data. Along that secure encryption transaction algorithm is implemented.

General Terms
WSN, Chaotic map, SET-IBS, SET-IBOOS

Keywords
Security, sensor network, protocols

1. INTRODUCTION
WSN is one among the popular and widely used network which enhances performance but serious concern is referred to be high security. The data containing related information should not be accessed by unauthorized person though it may be important one. These concerns are relevant to the wireless sensor environment in which anyone can overhead the message sent. So for more convenience, system may appeal to the users if it is not secure. To overcome these conflicts, researches in Wireless Sensor Network several security protocols have been implemented that is needed by the network. TinySec[2] and TinyECC[3] are examples of such protocols. In general security is considered to be more costly. It costs more in sensor network because of the small amount of resources in the sensor nodes. Those should be properly utilized by the available resources. Consider as eg, if a device doesn't influence needed storage in order to implement the particular protocol that influence less storage memory which is also less secured.

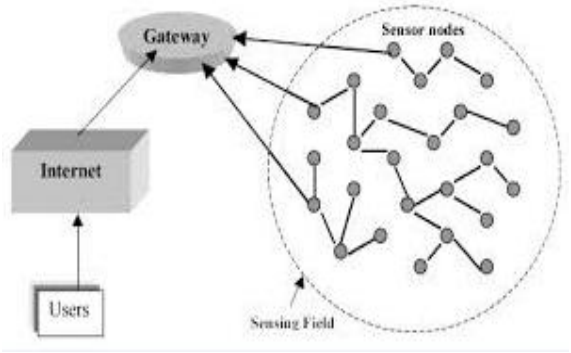

Figure 1: Sensor Node with Sensing Field

Unless encryption algorithms more ways are there in order to enhance security in wireless sensor networks. To encrypt plaintext multiple times with similar key and to produce different cipher text, various modes of operations are ensured. To guarantee the authenticity and data integrity, message authentication code algorithms are used. For security purpose, the encryption algorithms mentioned, modes of operation and authentication code algorithms are taking part in this paper. Hashing, symmetric and asymmetric key are the data encryption algorithms.

2. REVIEW OF WSN
In Wireless sensor networks, techniques like symmetric key algorithm and hash based algorithm are introduced which are discussed in research papers [4], [5]. These techniques are not combined with the sensor node that compromise attacks. An attacker/hacker consists of key with combination of single sensor node In those algorithms, every authentication key which is assumed to be symmetric are shared on the nodes which are referred as clusters. A polynomial code is assumed to be secret which depends on techniques named message authentication functions are discussed in [6]. This method function represents the security information with the theories on the secret sharing threshold, in which the threshold by the help of polynomial degree is calculated. Polynomial evaluation is used to authenticate the nodes present intermediately though the transferred messages with the threshold units are applied.

The enhanced elliptic curve cryptography (ECC) development relies on the schemes of public key that provides advantages on the memory consumption, complicacy of message and protection because simple and efficient management of key is provided by public key techniques adapted[9]. The secret polynomial should be reconstructed because when the transferred message count is greater than the assigned

threshold point, the polynomial degree should ensure the system to damage continuously. Thereby the complexity and the threshold among the attacker should be boost up and the polynomial should develop the noise randomly referring to perturbation factor [7] known as polynomial count coefficient. By using code schemes of error correction, the perturbation factor added to the nodes can be erased entirely[8]. Messages are sent with the private key of sender along with the message's digital signature with the help of public key techniques.

Security of wireless networks is the highest difficulty that provides limited resources [11][13][18]. Wireless sensor network has been improved in multiple ways as network of large scale. Its specified characteristics and intense classification enhances that if sensor fails, the tolerating rate of errors is improved which helps in gathering the information accurately. Applications like military, detection of fire, chain supply management, syndrome surveillance automation of energy, visual enablement, gaming technology, administration of building, other commercial environmental observation and home appliances etc influences this technology. Security and resource conservation is also implemented in wireless sensor network using cryptographic algorithm [19] [20].

3. EXISTING METHODS

3.1 Symmetric Key Block Cipher for Sensor Network

In this paper[1] authors proposed that in symmetric key encryption process, network protocol design should explore cost efficiency in which the amount of key transmitted is reduced. Using sensor node's virtual energy value first key generation is made with the help of dynamic key approach. Then to perform cryptography for data, RC5 algorithm is used. By using TCP/IP protocol layer the data packet that are encrypted is passed over the network. In order to obtain block cipher algorithm's advantage in insecure path of wireless sensor network, overall performance is evaluated for the implementation purpose. This algorithm helps to meet the computational cost that achieves the benefit of work that is more flexible to possible attacks.

3.2 Security Protocol SPINS

In this paper[12] authors proposed LEACH-C protocol to achieve security and efficiency for wireless sensor networks. Methods consisting of Public key and secret key cryptographic techniques are used in the proposed system. Using public key cryptographic scheme, session key is delivered among sensor nodes in order to improve the network security and also to use less amount of energy. To aggregate the data in network plain method is used in turn which is compared with public key cryptography with data aggregation process.

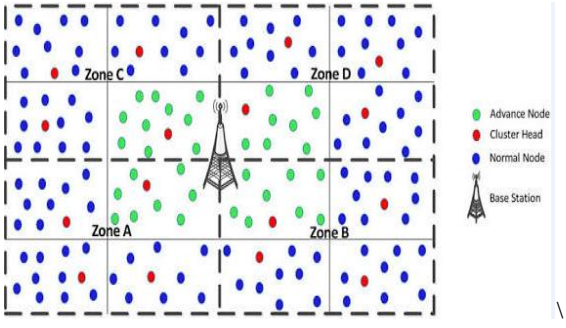

Figure 2: LEACH-C Protocol

As a result of the proposed scheme, energy efficiency is achieved high compared with other two schemes (i.e secret data aggregation and network data aggregation) without affecting the security environment during transfer of data.

3.3 Message Authentication Code using Different Cryptographic Techniques

In this paper[2] authors proposed Message Authentication Code (MAC) which uses the technique that promotes feasibility for the sensor network in turn. Symmetric key and asymmetric key cryptography are the techniques investigated by the proposed system. Different types of encryption techniques are compared. They are ciphers (stream cipher and block cipher) and hashing techniques. Compared to computation and communication costs with symmetric key, public key is expensive and not efficient in terms of energy. Techniques of symmetric key are selected and by comparing hash techniques with different attacks it is concluded that while comparing with block cipher it provides good security mechanisms. Although it acquires more overhead and uses more memory whereas stream cipher includes lower security when compared to block cipher. Overhead in packets also takes place in stream cipher for the purpose of encryption process.

3.4 Secure Network Layer ContikiSec

In this paper[15] author proposed a network layer designed for the Contiki Operating System named contikisec. ContikiSec consist of 3 modes providing security which starts from confidentiality and integrity. Then the configurable design expand to confidentiality, authentication and integrity. In order to balance security and to consume low energy ContikiSec has been developed. This design was based on the evaluation of performance of security constraints that are present in existing system which is contributed in the proposed paper. For wireless sensor network evaluation is performed in which Modular Sensor Board hardware platform with contiki inbuilt. Contiki is an OS which is highly portable and open source that is widely used in WSNs.

3.5 Light Weight Block Cipher KLEIN for Wireless Sensors

In this paper[14] author proposed KLEIN which is lightweight block cipher's new family. This was designed for wireless sensors and RFID tags which is resource-constrained. For low resource applications of wireless sensor networks, the design aims to develop a secure cipher which is more practical. Block cipher's security and performance analysis is considered complex.

3.6 Public Key Cryptography with Direct Diffusion Protocols

In this paper[17] author presents an encryption scheme suitable for direct diffusion protocols. Public-key cryptography has been observed to suffer from high computational complexity and overhead. The symmetric-key schemes can be utilized more efficiently in order to provide more security. In between the nodes of a network, secure communication is ensured by the symmetric-key function whereas data delivery security between the source is ensured by the public-key function. Kalpana (2012) also proposed PKC for minimizing the energy consumption in encrypting data packets. The scheme is suitable for data centric routing protocol. The key idea behind the scheme is that it uses PKC and SKC in the encryption/decryption process. The proposed security scheme overcomes the drawbacks of both protocols

(i.e.) public key and symmetric key. It uses secure hashing algorithm and this will incur additional (h) bits to be sent along with the original data packet guarantee for authenticity or the integrity. Scalable Encryption algorithm is used instead of RC5.

3.7 LU Matrix Scheme of Key Pre Distribution

In this paper[16] authors proposed pre distribution of key referred as LU matrix scheme that to be used for distribution of key between nodes in a network. Mutual authentication is provided between node to node which is the output of proposed LU matrix scheme that is key pre-distribution technique. In the sensor network between any two sensor nodes it also ensures to find common key. RC5 is considered to be more efficient and flexible cryptographic algorithm. In order to tradeoff strength in security with consumption of power and overhead computation many parameters (key size, block size, number of rounds) can be adjusted. RC5 sends the encrypted information after distribution of key.

4. SECURITY SCHEMES AVAILABLE

1. JAM security scheme causes denial of service attacks referred as jamming attack in traditional wireless sensor network architecture. Feature detected is avoiding the region jammed with the help of neighbor nodes which are coalesced.
2. On security communication causes spoofing attack such as information or data in WSN architecture. Feature detected is management of resource efficiently, protection of network in case if something wrong happens.
3. In traditional wireless sensor networks, TinySec and TESLA[5] scheme causes spoofing of data and replay attacks of messages.
4. Resource Testing of radio, Pre distribution of random key generation causes Sybil attack in WSN. Registration procedure, verification of position and code attestation, random key pre distribution are used to detect Sybil entity.
5. Random key pre distribution[11], [13] causes spoofing and transit information attacks. This scheme provides authentication measures and resilience of the network.
6. Verification of bidirectional data, Multi-path and multi-base station routing which is used to adopt secret sharing causes hello flood attack.
7. Wormhole based scheme[19] causes spoofing of information which takes place in dense wireless sensor network with more number of sensor nodes. During transmission, detect the duplicates.

5. SUMMARY

In this paper we have discussed various security methods available and discussed various security schemes available in order to avoid insertion of false information and to secure the data transmission in between sensor nodes.

6. REFERENCES

[1] Mr. Bhavin N Patel, Ms. Neha Pandya, “Secure Data Transfer using Cryptography with Virtual Energy for Wireless Sensor Network”.

[2] Sadaqat Ur Rehman, Muhammad Bilal, Basharat Ahmad, Khawaja Muhammad Yahya, Anees Ullah, Obaid Ur Rehman, “Comparison Based Analysis of Different Cryptographic and Encryption Techniques Using Message Authentication Code (MAC) in Wireless Sensor Networks (WSN)”.

[3] Jian Li, Yun Li, Jian Ren Jie Wu, “Hop by Hop Message Authentication and Source Privacy in Wireless Sensor Networks”.

[4] F. Ye, H. Lou, S. Lu and L. Zhang, “Statistical enroute filtering of injected false data in sensor networks”.

[5] S. Zhu, S. Setia, S. Jajodia and P. Ning, “An interleaved hop by hop authentication scheme for filtering false data in sensor networks”.

[6] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, “Perfectly secure key distribution for dynamic conferences”.

[7] W. Zhang, N. Subramanian and G. Wang, “Lightweight and compromise resilient message authentication in sensor networks”.

[8] H. Wang, S. Sheng, C. Tan, and Q. Li, “Comparing symmetric key and public key based security schemes in sensor networks”.

[9] ChungKuo Chang, J. Marc Overhage, Jeffrey Huang, “An Application of Sensor Networks for Syndromic Surveillance”.

[10] Matthew N. Vella, “Survey of Wireless Sensor Network Security”.

[11] Xiaojiang Du, North Dakota State University and HsiaoHwa Chen, National Cheng Kung University “Security in Wireless Sensor Networks”.

[12] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J. D. Tygar, “SPINS: Security Protocols for Sensor Networks”.

[13] SungChul Jung , HyoungKee Choi, “An Energy aware Routing Protocol Considering Link Layer Security in Wireless Sensor Networks”.

[14] Zheng Gong1, Svetla Nikova1;2 and Yee Wei Law, “KLEIN: A New Family of Lightweight Block Ciphers”

[15] Lander Casado and Philippas Tsigas, “ContikiSec: A Secure Network Layer for Wireless Sensor Networks under the Contiki Operating System”.

[16] Suraj Kumar Khuraijam, Dr Radhika K R (2013), “A Novel Symmetric Key Encryption Algorithm Based on RC5 in Wireless Sensor Network”.

[17] Shanta Mandal And Rituparna Chaki(2012),”A Secure Encryption Logic For Communication In Wireless Sensor Networks”.

[18] Md. Anisur Rahman and Mitu Kumar Debnath, “An Energy Efficient Data Security System for Wireless Sensor Network”.

[19] Mohammad ALRousan, A.Rjoub and Ahmad Baset, “A low energy security algorithm for exchanging information in wireless sensor networks”.

[20] Y.W. Law, S. Dulman, S. Etalle, P. Havinga (2002), “Assessing security critical energy efficient sensor network”.

[21] I. Ituen and G. Sohn, “The Environmental Applications of Wireless Sensor Networks”

[21] Wang, X. and Yu, H., "How to Break MD5 and Other Hash Functions".