International Journal of Research in Advanced Engineering and Technology
ISSN: 2455-0876; Impact Factor: RJIF 5.44
Received: 25-05-2020; Accepted: 10-06-2020; Published: 26-06-2020
www.newengineeringjournal.in
Volume 6; Issue 2; 2020; Page No. 04-07

A noble security scheme for wireless sensor network

Taruna Sikka[1], Shikha[2]
[1-2] Assistant Professor, Satpriya Group of Institutions, MD University, Rohtak, Haryana, India

Abstract
Nowadays, the technology of the wireless communication is replaced by the wires. WSN (Wireless Security Networks) is also a part of the wireless communication technology as it provides us the internet with high speed. As the other technology of the wireless communication technology are not secured or safe. Various issues related to security are reported in WSN (Wireless Security Networks). In this, authentication models and authorization network resources are used to save or protect it from the unauthorized use. The encrypted mechanisms or the authentication both are proposed for WSN (Wireless Security Networks) security but still the WSN networks were not secured fully or these are also under the attacks like Passive attack, Active attack, Insider attack, close in attack, distributed attack. In this, we proposed a security scheme for the increase in its capability and the functions of the existing models. Also, in this, we will use scythe tool for the verification of our proposed security scheme.

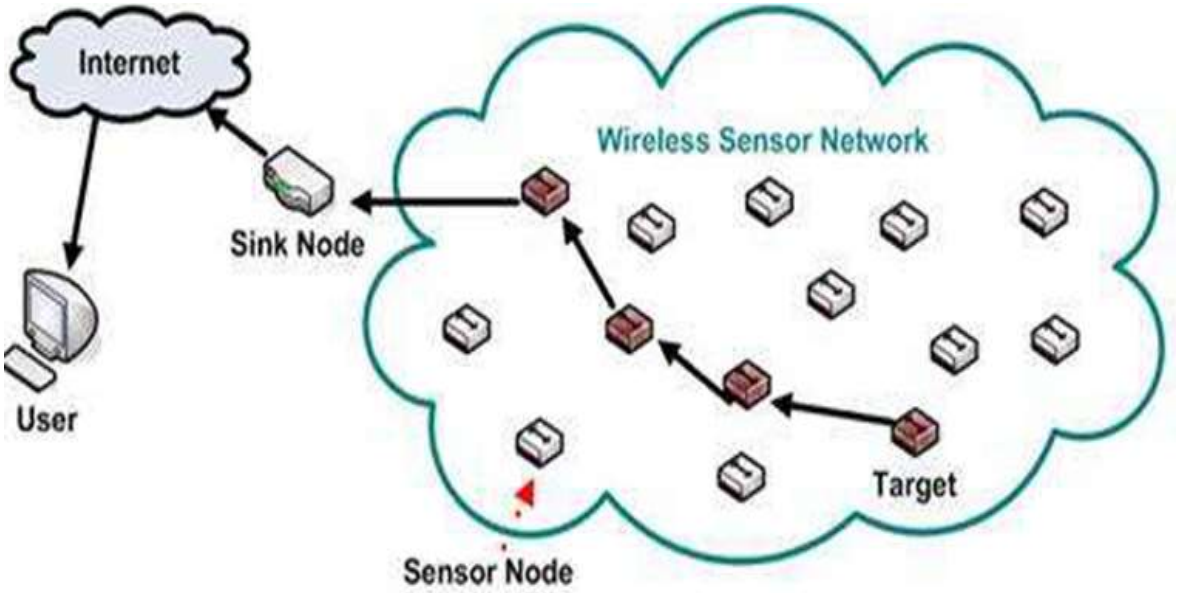
Keywords: wireless, models, Nowadays, WSN

1. Introduction

The WSN (Wireless Security networks) is used for the reduction of the consumption of energy to a level which is suitable for many applications. Our paper has considered the ease in the scenario of disaster relief, whereas the wireless security / sensor on the physical conditions within road tunnel. In this scenario, it is impossible to recharge. In this, Radio Power Control is very much important which helps us to increase the network for lifetime. The energy utilization for off-the-shelf sensor/ security nodes is up to 70% and the transmission power is accountable for that. For example, if we keep the pass on power under control it helps us to reduce the probability of the packet collision, which leads to retransmission of packets waste, which consume more energy.

Most wireless communication networks are basically based on the radio waves through which the medium of the network is open for interception. As the network of the security always plays an important role in presentation of the networks.

WSN (Wireless Security Networks) is a wireless networks or technology which is inherently open for Interceptions and in this, the security is a big concern. For the end, users security concerns it requires the core networks, application servers and everywhere in between. To secure the WSN (Wireless Security Network) from the threats, there are various security Management that are other or different from other old technologies. In this, the scheme which is proposed is more reliable and secured.



***Source*:** Adapted from http://irmadwmulyanti.it.student.pens.ac.id/index5.html

Fig 1: Wireless sensor network

2. Different types of wireless security network system

- **Terrestial System:** This **c**ommunication uses the transmitters and receivers that are based on earth and which resembles the satellite dishes. It uses low-ghz range and it limits the communication to the line-of-sight.
- **PC and Cellular System:** It uses radio communication technology, it also divides region covered into the multiple geographic areas. In this, every area has low transmission power or radio relay anteena which is used to relay calls from one area to the next area.
- **Free Space Communication:** It use visible and invisible light for the communication purpose. Line of sight propogation is used in this which limits the physical positioning of the communication devices.
- **Radio and Spread Spectrum Technology:** In this, the wireless local area network (LAN) uses a high-frequency radio technology which is similar to digital cellular and a low frequency radio technology. These are used to spread the spectrum technology which is used to enable the communication between the multiple devices in a limited area.

3. Types of Attacks in Wireless Networks

- In this, the classes of attacks includes the passive monitoring of the communication, active network attacks, close-in attacks, exploitation by the insiders, and the attacks through service provider.
- The information systems and the networks offer the attractive targets and it should be resistant to attack from the full range of the threat agents, from the hackers to the nation states. A system must be able to limit the damage and the recover the rapidly when the attacks occurred.
- **Five types of Attacks**
- **Passive Attack:** The passive attack monitors the unencrypted traffic and it looks for the clear text passwords and the sensitive information that can be used in the other types of attacks. It includes the traffic analysis, monitoring of the unprotected communications, decrypting weekly encrypted traffic, and capturing the authentication information such as passwords. The passive interception of the network operations enables the adversaries to see the upcoming action. These attacks also results in the disclosure of the information or the data files to the attacker without the consent or of the knowledge of the user.
- **Active Attack:** In this attack, the attacker tries to bypass or to break into the secured systems. This can also be done through the stealth, viruses, worms or the Trojan horses. The active attacks includes the attempts to thecircumvent or the break protection features, to introduce the malicious code, and to steal or modify the information. These attacks are the attacks which are mounted against the network backbone, exploit the information in transit, electronically penetrate the enclave, or the attack which is an authorized remote user during the attempt which is used to connect to an enclave. These attacks results in the disclosure or discrimination of the data files, Dos and the modification of data.
- **Distributed Attack:** This attack required that the adversary introduced the code, such as back-door and the Trojan horse program, to trusted component or the software that will later to be distributed to the other companies and to the users distribution attacks which focus on o the malicious modification of software and hardware in the factory or during the distribution. Distributed attack introduced the malicious code such as back door to a product or to gain unauthorized Access to the information or to the system function.
- **Insider attack:** The insider attack involved someone from the inside or not from the outside, such as disgruntled employee, which attacks the insider network attacks which can be malicious or not a malicious. In this, insiders intentionally eavesdrop, damage information, steal or use of the information in fraud manner. And when there is no malicious attacks typically it results from the carelessness, lack of the knowledge or the intentional of security for few reasons for performing the task.
- **Close-in attack:** This attack involved someone's attempting to get close physically to the components of network, systems and data in order to learn about the network. This attack consists of individuals attaining the close physical proximity to the systems, networks or the facilities for the purpose of gathering, modifying or denying to access the information. In this, the physical proximity achieved through the entry to the network, open access or to the both.

4. Previous Work

HMAC

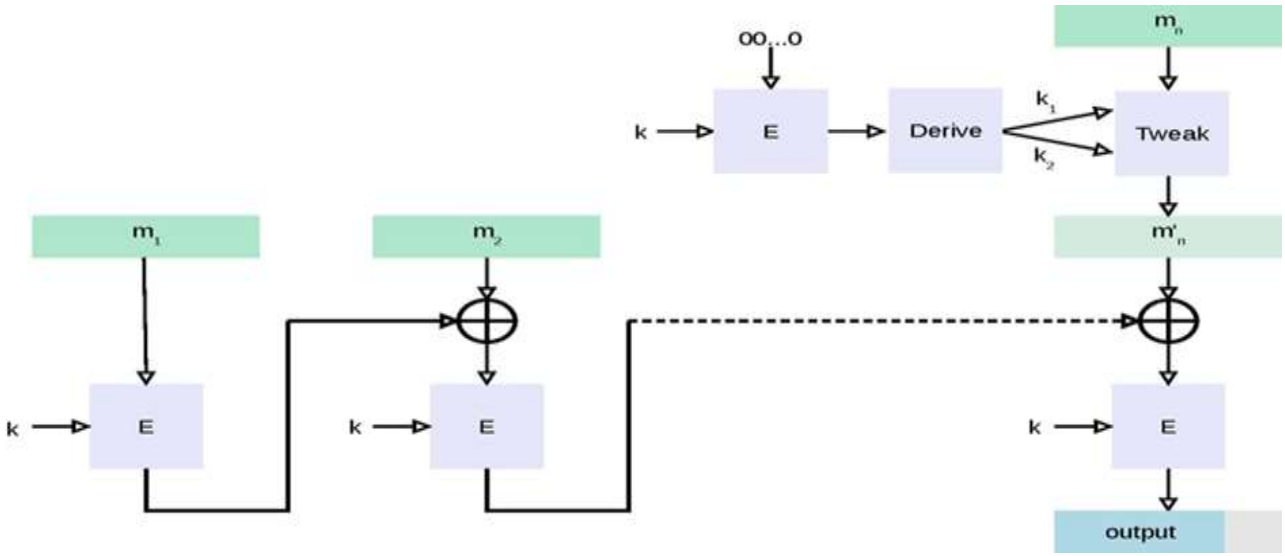
In cryptography, an HMAC (sometimes expanded as either keyed-hash message authentication code or hash-based message authentication code) is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message.

OMAC

One-key MAC (OMAC) is a message authentication code constructed from a block cipher much like the CBC-MAC algorithm. Officially there are two OMAC algorithms (OMAC1 and OMAC2) which are both essentially the same except for a small tweak. OMAC1 is equivalent to CMAC, which became an NIST recommendation in May 2005. It is free for all uses: it is not covered by any patents. [1] In cryptography, CMAC (Cipher-based Message Authentication Code) is a block cipher-based message authentication code algorithm. It may be used to provide assurance of the authenticity and, hence, the integrity of binary data. This mode of operation fixes security deficiencies of CBC-MAC (CBC-MAC is secure only for fixed-length messages).

The core of the CMAC algorithm is a variation of CBC-MAC that Black and Rogaway proposed and analyzed under the name XCBC [3] and submitted to NIST.[4] The XCBC algorithm efficiently addresses the security deficiencies of CBC-MAC, but requires three keys. Iwata and Kurosawa proposed an improvement of XCBC and named the resulting algorithm One-Key CBC-MAC (OMAC) in their papers. [5] They later submitted OMAC1, [6] a refinement of OMAC, and additional security analysis. [7] The OMAC

algorithm reduces the amount of key material required for XCBC. CMAC is equivalent to OMAC1.



***Source*:** Adapted from https://en.wikipedia.org/wiki/One-key_MAC.

Fig 2: Block diagram of HMAC

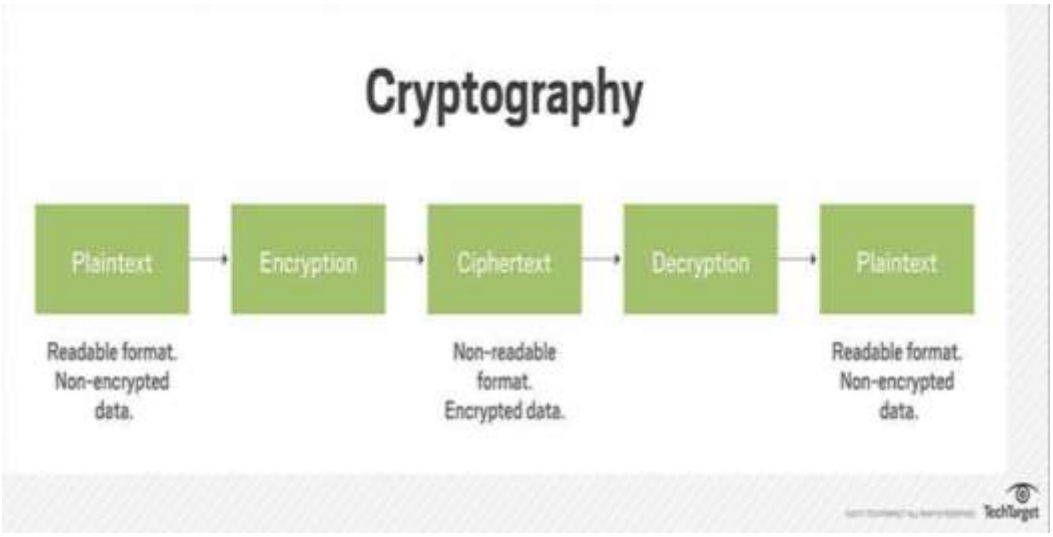
To generate an ℓ-bit CMAC tag (*t*) of a message (*m*) using a *b*-bit block cipher (*E*) and a secret key (*k*), one first generates two *b*-bit sub-keys (k_1 and k_2) using the following algorithm (this is equivalent to multiplication by *x* and x^2 in a finite field GF (2^b)). Let ≪ denote the standard left-shift operator and ⊕ denote bit-wise exclusive or:

Difference Between HMAC and OMAC

The main difference between MAC and HMAC is that MAC is a tag or a piece of information that helps to authenticate a message, while HMAC is a special type of MAC with a cryptographic hash function and a secret crypto Graphic key.

Cryptography

When transmitting data over the network, it is important to use a mechanism to secure the data. For example, in an online transaction, the user's credit card information is transmitted over the internet. There is a possibility for a hacker to steal this personal information. Therefore, when transmitting confidential information, it is important to use a data protection method. One such method is cryptography. It hides the real information when they are transmitted over the network.



Source: Adapted from https://searchsecurity.techtarget.com/ definition/encryption.

Fig 3: Block diagram of cryptography

5. Proposed Work

In this proposed work, the mutual authentication process between BS & MS in which MS&BS authenticate each other before the exchanging of the information. The proposed work or the proposed security scheme is that in which the exchange of the information occurs between BS & MS which will take place in few steps-

- Step-1:- In this, the MS initially wants to set a communication link with the BS, it sends an initial authentication message to BS. MS-BS: MS Cert (WTLS), Nonce-1(MS) and TS-1(MS).
- Step-2:- In this, MS sends the authentication request message to BS. MS-BS: MS Cert, Nonce-2(MS), TS-2(MS), Capb, SAID, DSign (MS).

- Step-3:- In this, the BS received the information/ message from MS and it checks the two conditions for the communication purpose. Firstly, TS-2(MS) is only valid then the BS proceeds and it will discarded the communication. Secondly, the BS validate for MS Cert, DSign(MS). If BS & MS both the identifications are valid then the BS will proceed and it will store the public key of the MS and Nonce-2 (MS), or it discard the communication.

BS-MS; ECC Encrypt-TS-1(BS), Nonce-2(MS), Nonce-1(BS), MS Public key (AK), Sequence No. (AK), Lifetime (Ak), SAID, BS Cert, Dsign (BS).

- Step-4:- In this, MS receives the message/information from BS and it validates TS-1(MS) & Nonce-2(BS). If TS-1(BS) and Nonce-2(BS) are valid then MS preceeds and it discards the communication process. MS validates again the BS Cert and the Dsign (BS) & if both are ready or validate as MS proceeds and discarded the process. After the validation the MS it will be decrypted the AK & the SAID List using the private key and it will save them along with the Nonce-1(BS). After that, the MS will start the key life timer and save the sequence no. (4-bit) of AK and it will established the association which is according to the SAID list. In this, the MS will send an acknowledged message to the BS.

MS-BS; Nonce-3(MS), Encrypted AK, Nonce-1(BS), MAC (MS).

- Step-5: In this, the MS sends request for Traffic Encryption Key to BS. Traffic Encryption Key is use for the data encryption and the messy. MS-BS; SAID, Sequence no. (AK), Lifetime (AK), OMAC-Digest.
- Step-6: In this, the BS receives the request of Traffic Encryption Key from MS, and the BS generates the Traffic Encryption Key & sends back to MS as Traffic Encryption Key replies the message. BS-MS; Sequence no. (AK), SAID, Encrypted Traffic Encryption Key, Lifetime Traffic Encryption Key, OMAC Digest.

Conclusion

In wireless sensor network security is as important as performance and energy efficiency for many applications (Park *et al*., 2005). Network security is important for many applications and areas. Additionally, wireless sensor network security is necessary for premise protection and surveillance, and the critical communities for instance, banks, railways, financial services premises, public utilities offices etc. To address this issue, scientist invents a new scheme which facilitates the organizations. Our paper proposed a new scheme which facilitates to minimize the time overhead by avoiding the in the key- distribution step. Additionally, suggested novel scheme has proposed a noteworthy development in the performance and energy effectiveness of the sensor nodes.

References

1. Liu D, Ning P. Establishing pairwise keys in distributed sensor networks: Proceedings of the 10th ACM Conference on Computer and Communications Security, 2003, 52-61
2. Erdo, Renyi. on random graphs I: Publ. Math. Debrecen. 1959; 6(9):290-297
3. Choi SJ, Youn HY. An Efficient Key Pre-distribution Scheme for Secure Distributed Sensor Network: The 2005 IFIP International Conference on Embedded and Ubiquitous Computing (EUC'2005), LNCS, 2005.
4. Stajano F. Security for Ubiquitous Computing: Jhon Wiley and Sons, ISBN 0-470-84493-0, 2002.
5. Cam H, Ozdemir S, Nair P, Muthuavinashiappan D ESPDA, Energy-efficient and secure pattern based data aggregation for wireless sensor networks: IEEE Sensor Networks, 2003.
6. Chan H, Perrig A, Song D. Random key pre-distribution schemes for sensor networks: IEEE Symposium on Security and Privacy. 2003, 197-213
7. Akyildiz IF, Su W, Sankarasubramaniam Y, Cayirci E. A survey on sensor networks: IEEE Communications Magazine. 2002; 40(8):102-114
8. Eschenauer L, Gligor VD. A key-management scheme for distributed sensor networks: Proceeding of the 9th ACM Conference on Computer and Communication security, 2002, 41-47
9. Park CW, Choi SJ, Youn HY. A Noble Key Pre-distribution Scheme with LU Matrix for Secure Wireless Sensor Networks. In: Hao Y. *et al*. (eds) Computational Intelligence and Security. CIS. Lecture Notes in Computer Science, 2005, 3802. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11596981_73
10. Anderson R, Kuhn M. Tamper resistance – a cautionary note: Proceeding of the Second Usenix Workshop on Electronic Commerce, 1996, 1-11