Authentication Protocol against Malicious Attack in Wireless Sensor Networks: A Review

Amit Kumar Sharma
ABES EC, GZB

Sunil Gupta
NIEC

Rashmi
ABES EC, GZB

ABSTRACT
Nodes in a sensor network may be lost due to malicious attack or either power loss. To extend the life time of the sensor network the novel Authentication Protocol is needed to overcome the internal attacks. In a defense scenario the advisory or intruder may directly deploy the malicious node or manipulate existing node to introduce malicious new node to the network. This paper focus on Novel Authentication Protocol to provide a security solution against known malicious attacks. It provides better authentication protocol for access control in the sensor network. We also emphasis on the confidentiality for the information access in between the sensor networks. In this paper we review secure WSN user Authentication Protocol and its several security weaknesses. According to our analysis of security our protocol as compare to security, computation and communication cost is scalable for application with higher security requirements. Our protocol is well designed for sensor nodes which typically have limited resources with better authentication procedure that use one way hash function and smart cards can be implemented efficiently.

Keywords
Authentication, Wireless Sensor Network, Smart Card, Security Attacks.

1. INTRODUCTION

Security allows WSNs to be used with assurance. Without security, the use of WSN is any application area would cause in undesirable consequences. Wireless sensor networks are rapidly gaining regard due to low cost solutions to a variety of real world challenges. The basic idea of sensor network is to disperse tiny sensing devices, which are able for sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some particular purposes like surveillance, environmental monitoring and target tracking.

Now a day's sensors can monitor pressure, temperature, humidity, soil makeup, noise levels, vehicular movement, and lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties. In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, as a result the memory, processing power and type of tasks affected from the sensors. To deal with the important security issues in wireless sensor networks this paper talk about cryptography, steganography and other basics of network security and their applicability. This paper investigate various types of threats and attacks against wireless sensor network to save manufacturing cost. A sensor node is usually built as a small device, which has limited memory, a low-end processor, and is powered by a battery. So during the design of any security solution we need to take care of resource constraints like limited energy, limited memory, limited computing power, limited communication bandwidth, limited communication range.

2. LITERATURE SURVEY

Krik H.M Wong [1] proposed a dynamic strong password based solution for access control problem and adapt a wireless sensor network environment. The proposed strong-password authentication approach imposes very light computational load and
requires simple operations, such as one-way hash function and exclusive-OR operations. He presents the design of the proposed scheme and discusses how to make use of the security features on MAC sub layer (Medium Access Control) based on the IEEE 802.15.4 specification. Analysis on security and communication costs is presented to evaluate the effectiveness of the proposed scheme. This scheme is divided into three phases: the Registration phase, the Login phase, and the Authentication phase.

Tseng et al.[2] proposed an improved dynamic user authentication scheme for WSNs. Their scheme is divided into four phases, i.e., the registration phase, the login phase, the authentication phase and the password change phase. The registration phase is performed only once via a secure channel. The login phase is executed whenever a registered user wants to retrieve sensor readings from a nearest sensor login-node. Then, she sends the query to the sensor login-node by using mobile devices. The authentication phase is started whenever the gateway receives user's login message forwarded from the sensor login-node. Upon receiving the message from the sensor login-node, the gateway checks user's authenticity and replies the checking result to the sensor login-node. The password change phase is started whenever the users want to change their password via a secure channel.

Lee-Chun Ko [3] proposed improved scheme by modifying Tseng et al.'s scheme. Note that the improved registration phase and password change phase are performed via a secure channel. This is the same assumption as Tseng et al.'s scheme. The proposed scheme is also divided into four phases which is explained in the following subsections, Improved Registration Phase, Improved Login Phase, Improved Authentication Phase, and Improved Password Change Phase. In addition to all the advantages of Tseng et al.'s scheme, his proposed novel scheme provides additional security strength as follows:

1) The proposed scheme is secure against replay attack. Since every message received at destination needs to be checked whether it is within the allowed time interval ΔT, replaying any messages will be noticed and dropped. This requires time synchronization mechanism for WSNs. A plenty of time synchronization schemes for WSNs have been proposed, interested readers may refer to for more details.

2) The proposed scheme is secure against forgery attack. The *U* is unable to forge any message that is sent from the *SN* to the *GW* and vice versa since the *U* does not have enough ability to compute *N* and *C*. This feature prevents any adversary from pretending to be a legitimate *SN* or the *GW*.

3) The proposed scheme achieves mutual authentication between the *U* and the *SN*, and between the *GW* and the *SN*, which is very important in many applications.

Lee-Chun Ko [3] have proposed a Novel Dynamic User Authentication Scheme for Wireless Sensor Networks first give a brief review of Tseng et al.'s dynamic user authentication scheme for WSNs. Then, he point out several weaknesses in Tseng et al.'s scheme and proposed a novel scheme, which not only inherits all the advantages of Tseng et al.'s scheme but also achieves mutual authentication and enhances its security strength. The performance comparison is also given. The proposed scheme stands similar assumptions as Tseng et al.'s scheme, and also uses hash functions and exclusive-or operations as underling cryptographic primitives. These two cryptographic primitives do not cost too much computational overhead and are considered affordable to the common sensor platforms. So we believe that the proposed scheme is also lightweight for wireless sensor networks.

Manik Lal Das [4] have proposed two-factor user authentication protocol for WSN, provides strong authentication, session key establishment, and achieves efficiency. Before issuing any queries to or access data from sensor network, the user has to register with the GW-node of the network. Upon successful registration, the user can submit query to the WSN at any time within a predefined or administrative configurable period. The basic idea of the protocol is that a user will receive a personalized smart card from the GW-node at the time of the registration process and then, with the help of user's password and smart card the user can login to the sensor/GW node and access data from the network The protocol is divided into two phases: Registration phase and Authentication phase. The protocol avoids many logged in users with the same login-id and stolen-verifier attacks, which are prominent threats for a password-based system if it maintains verifier table at the GW-node or sensor node. In addition, the protocol resists other attacks in WSN except the denial-of-service and node compromise attacks.

Hui- Feng Huang and Ya-fen Chang [5] proposed an Enhancement of two factor user authentication in wireless sensor network. Das's[4] proposed a two-factor user authentication scheme in wireless sensor networks. They claimed that this scheme provided efficiency, strong security, and user anonymity property. However, he find that Das's scheme is still vulnerable to masquerade attack and cannot achieve user anonymity. He proposes an improvement to remedy the weakness of Das's scheme. And second the security analysis of the proposed scheme is made. In the proposed scheme he used a symmetric key known to only the gateway node and a secure parameter generated by gateway node. The improved scheme have four phases: first is registration phase, second login phase, third is verification phase and fourth is password change phase. His improved method provides: no password table is required by gateway node, user can freely choose their own password, user may update their passwords after registration phase, user anonymity property is provided.

Muhammad Khurram Khan, and Khaled Alghathbar [6] proposed Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks. He shows that the M.L. Das-scheme [4] has some critical security pitfalls and cannot be recommended for real applications. He point out that in his scheme: users cannot change/update their passwords, it does not provide mutual authentication between gateway node and sensor node, and is vulnerable to gateway node bypassing attack and privileged insider attack. To overcome the inherent security weaknesses of the M.L. Das-scheme, he proposes improvements and security patches that attempt to fix the susceptibilities of his scheme. The proposed security improvements can be incorporated in the M.L. Das-scheme for achieving a more secure and robust two-factor user authentication in WSNs.

He proposes security improvements over the scheme of M.L. Das and performs analysis of his security patches includes Introducing Password Change Phase, Protection against Insider Attack, Overcoming GW-node Bypassing Attack and Providing Mutual Authentication.

He proposes not to share the same secret parameters with sensor node and user, and that every entity has its own secret parameter or key. Here, he suggest that the GW-node should only share sensor node with user id and there should be another secret parameter, which should only be known to the GW-node and sensor nodes, and can be stored in sensor nodes before their deployment in the field. These sensor nodes are responsible to respond users for their queries.

Although, in the proposed security patch, the introduction of one more secret parameter creates storage overhead on the GW-node, but its benefits are two-fold and cannot be overlooked. The first benefit, as defined previously, is to overcome the GW-node bypassing attack, while the second benefit is the ease of secret parameter (key) updating incase of compromise of secret parameters by an adversary.

His scheme provides protection against insider attack, gateway node bypassing attack, password change/update option, and achieves mutual authentication between gateway and sensor nodes, which require few more hashing operations than [4] to enhance the security of overall authentication system. Hence, the computational overhead of the proposed scheme are not too high, but the scheme contains several enhanced security features, which are indispensable for implementing a reliable and trustworthy remote user authentication scheme in the WSN environment.

Binod Vaidya, Dimitrios Makrakis, Hussein T. Mouftah **[7]** proposed an Improved Two-factor User Authentication in Wireless Sensor Networks. This new scheme can overcome pitfalls in Das's [4] and Khan-Algahathbar's [6] schemes as well as provide robustness and higher level of security. As stated in Das's scheme [4], WSNs are deployed in a confined area, which could be divided into different zones. Authorized users can access WSN using their mobile devices (e.g., notebook, PDA). Prior to getting access to WSN, the user has to register with GWN. Only after successful registration the user can send query to the WSN at any time within a predefined or administrative configurable period. The basic idea of the protocol is that during registration phase, a user

receives a smart card from GWN and during login-authentication phase, the

user can login to the sensor/GWN and access data with the aid of the user's password and smart card. His main goal is to reduce potential problems caused by illegitimate users and compromised smart cards. In this regard, he proposes a smart-card based password user authentication scheme to satisfy the following requirements:

- The scheme should provide protection against various attacks that are based on the use of a stolen smart card.
- The scheme should provide mutual authentication between GWN and SN-node in order to prevent forgery attacks.
- The scheme must be lightweight and efficient in terms of communication and computation in order to reduce the energy consumption of sensor nodes as typical sensor nodes are resource constraint and have limited energy.
- The scheme should be a zero-knowledge password protocol. That means it allows a claimant to authenticate to a verifier without revealing password.
- The scheme should have provision to change password and update other parameters. In this scheme, there are three basic phases – registration, login/authentication and password change.

Registration phase begins when a user (UID) submits its identity and hashed password to the remote system after that login/authentication phase is invoked when UD wants to perform some query to or access data from the WSN and in last Password Change Phase will be initiated, the password could be changed without any interaction with GWN. During the password-change phase, a registered user UD can change the password and update parameters in the smart-card accordingly. This helps to alleviate scalability problems and facilitates user friendliness. After receiving the current password pwi and the new password pwni, the smart card will first confirm the validity of current password.

He also observed that the computational overhead of the proposed scheme is insignificantly higher than those of aforementioned schemes due to the fact that the both GWN and SN-node need either same or only slightly higher hash computations than previous schemes. Furthermore, the proposed scheme incorporates numerous additional security features, which make it a more robust and secure two-factor user authentication in the WSN environment. However, his scheme does not provide session key agreement and mutual authentication between user and sensor node/gateway node.

Da-Zhi Sun, Jian-Xin Li, Zhi-Yong Feng, Zhen-Fu Cao, Guang-Quan Xu[8] their crucial idea is that the GW-node distributes the different secret key for each user id and each sensor node to avoid GW-node impersonation attack and the GW node bypassing attack. They can intuitively see that user id cannot impersonate the GW node without its secret key. For the same reason, the adversary owning one sensor node secret key is difficult to bypass the GW-node to access other sensor-nodes without their corresponding secret keys.

Their proposed scheme composes of three phases, that is, the registration phase, the password change phase, and the authentication phase. In the registration phase the GW-node Generates the initial password for user id.

This design not only well adapts to the style of the card issuer but also thwarts the privileged-insider attack. After receiving the smart card, user id is able to immediately change the initial password by using the password change operation. In password change phase user can freely change his password without any interaction with the GW-node. Because the GW-node cannot touch any user's password information, this design prevents the possibility of the privileged-insider attack. The authentication phase is invoked when user wants to perform some query to or access data from the WSN.

Table- 1 comparative Study

Phase	Wong	Tseng	Lee	M.L. Das	Hui- Feng	Khan-Algahathour	Binod Vaidya	Da-Zhi Sun
Registration	$2T_H+1C_{MH}$	$1T_H+1C_{MH}$	$2T_H+2T_{XOR}+1C_{MH}$	$2T_H+1T_{XOR}+1C_{MH}$	$3T_H+1T_{XOR}+1C_{MH}$	$3T_H+3T_{XOR}+1C_{MH}$	$5T_H+3T_{XOR}$	$2T_H+1T_{XOR}$
Login	$2T_H+2T_{XOR}+1C_{MH}$	$2T_H+2T_{XOR}+1C_{MH}$	$3T_H+3T_{XOR}+1C_{MH}$	$3T_H+1T_{XOR}+1C_{MH}$	$3T_H+1T_{XOR}+1C_{MH}$	$6T_H+2T_{XOR}+1C_{MH}$	$6T_H+2T_{XOR}$	$2T_H+1T_{XOR}$
Authentication	$1T_H+1T_{XOR}+1C_{MH}$	$2T_H+2T_{XOR}+1C_{MH}$	$11T_H+13T_{XOR}+1C_{MH}$	$5T_H+2T_{XOR}+1C_{MH}$	$5T_H+2T_{XOR}+1C_{MH}$	$7T_H+4T_{XOR}+IC_{MH}$	$7T_H+4T_{XOR}$	$5T_H+$
Password Change	_____	_____	_____	_____	$2T_H+1T_{XOR}+1C_{MH}$	$2T_H+2T_{XOR}$	$6T_H+6T_{XOR}$	$2T_H+1T_{XOR}$
Total Cost	$5T_H+3T_{XOR}+3C_{MH}$	$5T_H+4T_{XOR}+3C_{MH}$	$16T_H+18T_{XOR}+3C_{MH}$	$10T_H+4T_{XOR}+3C_{MH}$	$13T_H+5T_{XOR}+4C_{MH}$	$18T_H+11T_{XOR}+4C_{MH}$	$24T_H+15T_{XOR}+4C_{MH}$	$11T_H+3T_{XOR}+4C_{MH}$

They only compare the proposed scheme with KA's [6] scheme, because both schemes employ similar cryptographic tools and attempt to achieve the same security goals. One distinction is that the proposed scheme is a nonce-based scheme, but KA's scheme is a timestamp based scheme. It is well known that the timestamp-based scheme requires that time clocks be both synchronized and secured. The preclusion of adversarial modification of local time clocks is difficult to guarantee in many distributed systems, for example, the WSNs. As a disadvantage, the nonce-based scheme needs one additional message exchange compared with the timestamp-based scheme.

They highlight two areas for future work. There is no appropriate formal model to examine the security of the user authentication scheme for WSNs and how to present a formal definition of the user authentication under the WSN setting and design the scheme, which can be reduced to satisfy the definition assuming the minimal cryptographic assumption.

3. COMPARATIVE ANALYSIS

Our analysis shows the effectiveness against the Sybil attack, the node replication attack, and the wormhole attack by including the security time stamp in our protocol, a new node is only allowed to join the sensor network during its time stamp length. After that it becomes an old node. Hence, malicious ‘‘new’’ nodes are prevented from joining the sensor network at the very beginning, because they do not have the proper bootstrapping time, and they are prevented from falsifying the latest security time stamp which does not match their certificates. The comparative study chart is as shown in table 1 shows the proposed framework has less computational cost and overhead as compare to the respective other protocol. Fig.1, 2,3,4,5 & 6 shows the comparative analysis on the base of cost and overhead of one way hash function and bit wise XOR function.

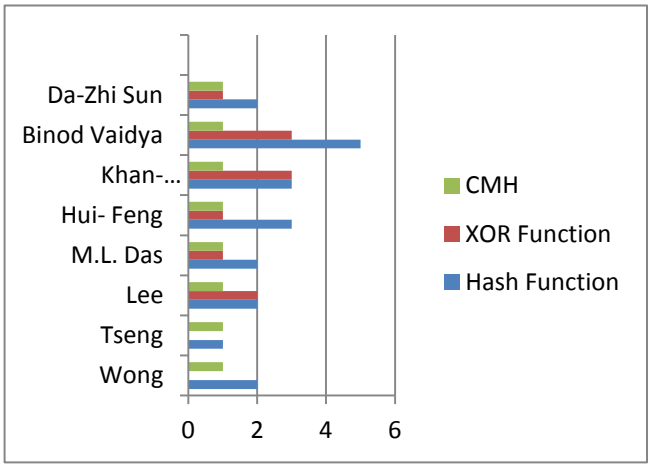

Fig.1 Registration Phase

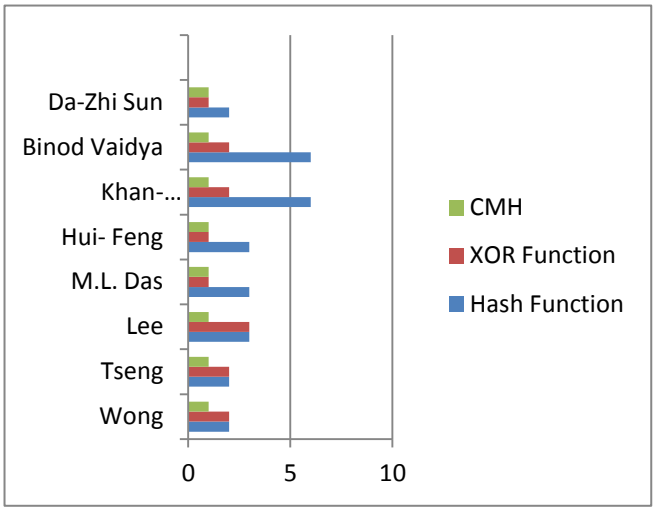

Fig 2 Login Phase

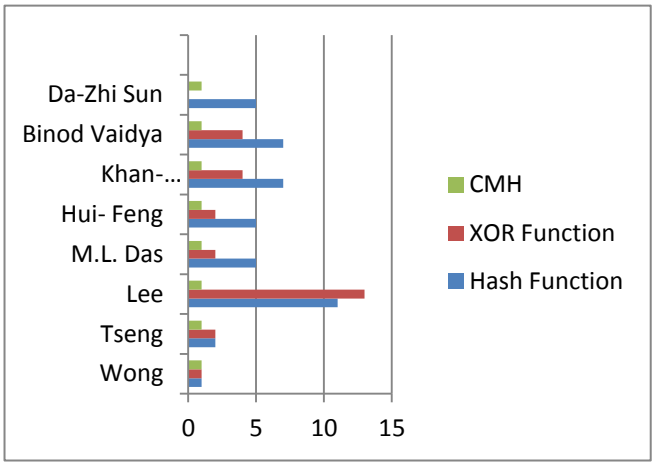

Fig. 3 Authentication Phase

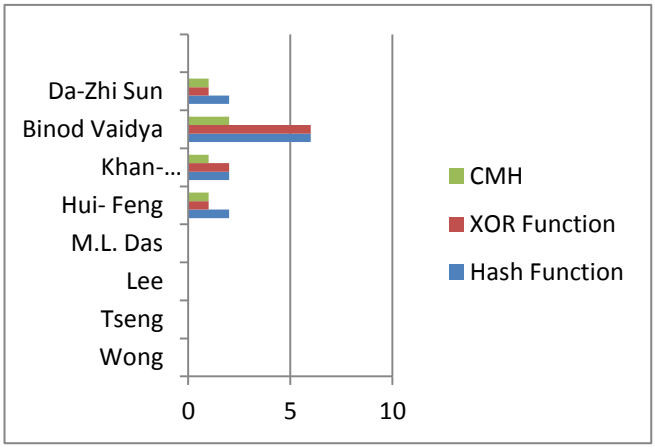

Fig. 4 Password Change

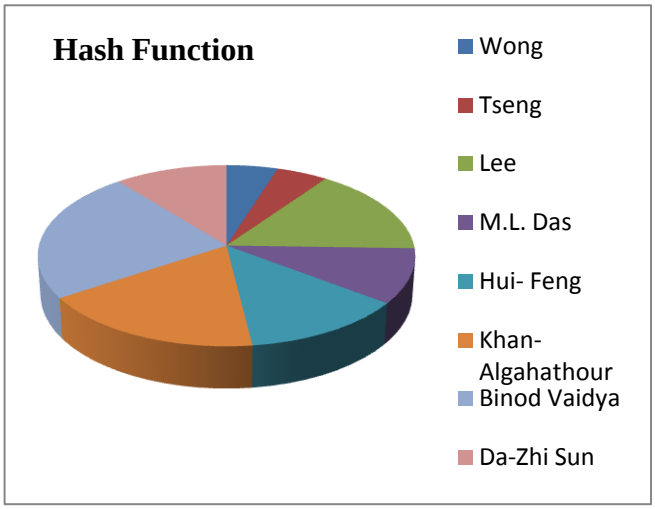

Fig. 5 Total Cost(Hash Function)

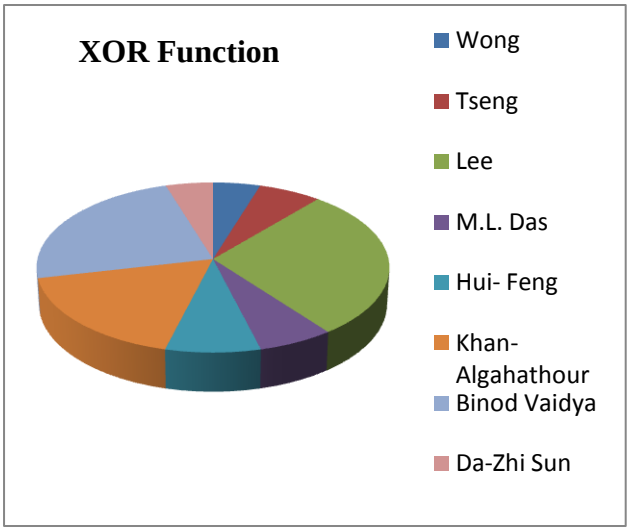

Fig. 6 Total Cost (XOR Function)

4. CONCLUSION

Wireless sensor networks are a unique class of mobile ad hoc network consisting of tiny low-cost resource constrained devices that have the ability to sense their environment, to in-process, to aggregate and to send the data to a destination. The deployment nature and limitations of the nodes resources as well as the wireless communication channel make sensor networks susceptible to a variety of new attacks in addition to the attacks which occur in wireless networks. Deployment of sensor networks has been envisioned in many sensitive applications such as military operations and health care. Despite advances in miniaturization and other developments in sensor networks occurring at a very fast pace, security within sensor networks has not gained significant interest.

5. REFERENCES

[1] Kirk H.M. Wong, Yuan Zheng, "A Dynamic User Authentication Scheme for Wireless Sensor Networks," Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), Computer Society,2006.

[2] Tseng, H.R.; Jan, R.H.; Yang, W. An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks. In *Proceedings of IEEE Globecom*, Washington, DC, USA, 26–30 November 2007; pp. 986-990.

[3] Lee-Chun Ko, "A Novel Dynamic User Authentication Scheme for Wireless Sensor Networks," IEEE ISWCS 2008, pp 608-612.

[4] Manik Lal Das, "Two-Factor User Authentication in Wireless Sensor Networks," IEEE transactions on wireless communications, vol. 8, no. 3, march 2009.

[5] Hui- Feng Huang and Ya-fen, "Enhancement of two factor user authentication in wireless sensor network," in sixth international conference on intelligent information hiding and multimedia signal processing,2010 IEEE .pp 27-30.

[6] M. K. Khan, and K. Alghathbar, "Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'", Sensors 2010, 10(3), pp. 2450-2459.

[7] Binod Vaidya, Dimitrios Makrakis, Hussein T. , "Improved Two-factor User Authentication in Wireless Sensor Networks," Second International Workshop on Network Assurance and Security Services in Ubiquitous Environments IEEE-2010, pp -600-606.

[8] Da-Zhi Sun, Jian-Xin Li, Zhi-Yong Feng, Zhen-Fu Cao, Guang-Quan Xu, "On the security and improvement of a two-factor user authentication scheme in wireless sensor networks," published in Springer-2012.