A Survey: Lightweight Cryptography in WSN

Shehnaz T. Patel
PG Scholar
Department of Computer Engineering,
SVM Institute of Technology
Bharuch, Gujarat, India
patelshehnazt@gmail.com

Nital H. Mistry
Department of Computer Engineering,
SVM Institute of Technology,
Bharuch, Gujarat, India
mistry_nital@gtu.edu.in

***Abstract*—A Wireless Sensor Network (WSN) is a wireless network which contains small sensor nodes to monitor physical or environmental conditions. When WSNs are deployed in inaccessible areas, the probability of occurring different types of attacks is very high. So the security of WSN becomes extremely important. As sensors have limited processing power, limited storage, low bandwidth, and energy; traditional security measures designed for the resource-rich networks such as LAN etc. are not suitable for the resource-constrained WSN. In presence of such limitations it becomes mandatory to devise lightweight security solutions for data transmission in WSNs. Because of problems in public key cryptography such as costly key computation, longer keys, key vulnerability to brute force attack, key distribution and maintenance, etc., it is not preferred for WSN. The less computation and low memory requirements of symmetric key cryptography with very short length of key (lightweight) justifies its use in WSN to achieve information security. Hence, this paper aims to study, discuss and analyze the Lightweight Cryptographic Algorithms Suitable for Wireless Sensor Networks.**

Keywords— Lightweight Cryptography, Confidentiality, Integrity, Authenticity, Availability, Data Freshness

I. INTRODUCTION

Wireless Sensor Network (WSN) is a network of sensors in which Sensor nodes are capable to sense the data and transmit it to the base station for analysis [1]. The sensors may be installed in a busy traffic area, under sea deployment, in a war field, in a house or an apartment on movable vehicles, in a chemical or biological hazardous field, etc. [1]. There are numerous real time applications of WSN such as Nature calamity forecasting, Greenhouse Monitoring, Battlefield surveillance, Industrial process monitoring and control, Machine health monitoring, Environment and habitat monitoring, Healthcare applications, Home automation, Traffic control and Vehicle Detection [1]. Generally WSNs are deployed in an inaccessible area; they are more susceptible to various attacks [2]. Attacks are classified in two types: Active attack and Passive attack [3]. In active attacks the attacker listens to and modifies the transmitted data. Denial of Service attack, node replication attack, routing attack etc., are few popular examples of active attacks [3]. In passive attacks the attacker only eavesdrops the transmitted data [3]. However, as WSN is a resource-constrained network, the security measures developed for the resource-reach networks such as LAN etc. are not suitable for the WSN [4]. Due to the limitations viz., communication in open and unguided media, deployment strategies, unattended deployed area it becomes quite easy to attack a WSN. Therefore the security of WSN becomes of utmost importance. For resource constrained nature of WSN it is important to devise lightweight security solution [4].Asymmetric and symmetric cryptographic solutions are available. Public key cryptographyis not preferred for WSN, because there are various problems such as costly key computation, longer keys, key vulnerability to brute force attack, key distribution and maintenance, etc [4]. Therefore, symmetric key cryptography with very short- length key is needed as a security solution that requires relatively less computations and memory requirement [4]. In this paper variouslightweight cryptographic solutions are surveyed.The rest of the paper is organized as follows. Section II presents background information of security goals. Section III presents various lightweight cryptographic methods for WSN. Finally concluding remarks are made in section IV.

978-1-5090-0051-7/15/$31.00©2015
IEEE DOI 10.1109/ICCN.2015.3

II. SECURITY GOALS IN WSNS

In an ideal world if every eligible node receives all the messages intended to it than we can ensure the security [5]. In the presence of resourceful adversaries, the security goal provides confidentiality, integrity, availability, and data freshness [5].

Confidentiality: Sensor node should not leak the data to other network. While communicating the data in the network, only intended recipient should understood the data. Cryptographic techniques are used to provide confidentiality.

Integrity: The intended receiver should receive data without any alteration in the data. Techniques such as message digest and MAC are used to provide integrity.

Authenticity: Data authenticity allows the receiver to verify that the data is sent by the authorized user. Cryptography mechanism like MAC is used to provide authenticity.

Availability: The services of a network should be available always to a legitimate node even in presence of attacks such as Denial of Service attack. Different mechanisms have been proposed by the researchers to achieve this goal.

Data Freshness: Receiver should receive the recent and fresh data and it should ensure that no attacker can replay the old data. The mechanism like nonce or timestamp should add to each data packet to achieve the data freshness.

III. LIGHT WEIGHT CRYPTOGRAPHY METHODS

This section provides and analyses various lightweight cryptography solutions available for WSN.

In [2], the authors have proposed Secured Query Processing Scheme (SQPS).SQPS provides security mechanism in a query driven environment. In this scheme clustered architecture for wireless sensor network based on LEACH protocol is considered. The Cluster Head (CH) selected using LEACH assigns a time slot for the members in the cluster. The member nodes transmit data to the CH and then CH forward the data to the base station. In SQPS system the base station generates the query messages and broadcast the query. When CH receives the query, it starts registration process for its member nodes. After completing the registration process CH forwards query messages to the member nodes. Depending on the nature of the queries, only specific member nodes send the response packets. As identity of all the member nodes is verified through registration phase, there is a very little chance for malicious nodes to steal identity of legitimate node and pass through registration phase. SQPS preserves authentication, integrity and data freshness along with defending replay attack. As symmetric key cryptography is used, the solution provided by the scheme is very lightweight.

The authors in [3] have proposed Modified Secured Query Processing Scheme (MSQPS). MSQPS provides security mechanism in a query processing environment. MSQPS provides basic security features such as confidentiality and integrity. It also protects from replay attack in presence of mote class attackers where attackers own same resources as ordinary nodes. Cluster head and member nodes are more vulnerable as compared to base station. That is why in all communications between CH and member nodes the key which is accepted at transmitting node is neither transmitted over wireless medium nor pre-deployed in the nodes, but again computed in receiving nodes. In MSQPS the security is provided to all phases of communication, i.e. from BS to CH, CH to MNs, MNs to CH and CH to BS. In MSQPS base station performs registration for CHs in addition to registration performed by CH for MNs. MSQPS is more efficient than SQPS.

The authors in [4] have proposed A Dynamic TDMA based Secured Query Processing Scheme (SQPS_DT). SQPS_DT is used to provide security in a query processing paradigm within WSN. The scheme provides authentication, data integrity, data freshness along with protecting replay attack. In Time Division Multiple Access method nodes share a bandwidth in time. CH creates TDMA schedule depending on the number of its MNs. A single 16 bit key is preloaded into all nodes of the network before deployment. This key is used to implement secure communication of the TDMA schedule between CH and MNs. The key is used only for authentication of TDMA schedule. It is not used further for implementing SQPS_DT scheme. All the MNs use their respective TDMA slots to communicate with the CH. In One variant of dynamic TDMA, scheduling algorithm dynamically reserves a variable number of time slots in each frame to accommodate data stream of variable bit rate, and it is used to establish the key information among nodes which ensures security of key. Another variant of dynamic TDMA is used for bandwidth saving. Communication between BS and CH uses Code Division Multiple Access (CDMA) and communication between CH and MNs uses Time Division Multiple Access (TDMA).

In [6] the authors have proposed a Light-Weight One-way Cryptographic Hash Algorithm (LOCHA). Authenticity of information is protected by cryptographic hash functions. Popular cryptographic hash algorithms such as MD5 and SHA1 cannot be used in energy starved network (WSN) as it requires high computational overhead. Keeping this in mind, a one way light weight hash algorithm with fixed and relatively small hash digest is developed for WSN. Low overhead operations such as MOD, SWAP are used to make the algorithm lightweight. Basic cryptographic properties of a one way hash function such as preimage resistance, collision resistance, and second preimage resistance are fulfilled by the algorithm.

Preimage Resistance is defined as for a given hash digest H it is computationally infeasible to find the message m such that h (m) = H where h (m) is the hash digest of m.Collision Resistance is defined as it is computationally infeasible to find any two inputs m1, m2 which results in same output, such that h (m1) = h (m2).Second Preimage Resistance is defined as for any given input m1, it is computationally infeasible to find second input m2 such that h (m1) = h (m2).

The authors of [7] have proposed an algorithm HIGHT. HIGHT is a lightweight algorithm and it is designed to be used by 8 bit computing devices (e.g. sensor node or RFID tag), for WSNs. It has 64-bit block and 128-bit key and 32-round iterative structure. HIGHT provides security against various attacks such as differential attack, linear attack, truncated differential cryptanalysis, saturation attack, etc. Simple operations such as XOR are used to make HIGHT speed optimized and size optimized. HIGHT is used on Mica2 motes. Mica2 mote is a sensor node with low power.

The authors in [8] have proposed a Byte-oriented Substitution-Permutation Network (BSPN). BSPN is a light weight block cipher which provides security to the sensor nodes in an energy limited environment of WSN. It protects from differential and linear cryptanalysis attack. BSPN has 8 byte block size, 64 bit (or large) key size and 8 rounds of operation. Each round includes add round key, substitution and linear transformation. BSPN uses fewest number of CPU cycles per byte and thus has the lowest computational energy cost.

The authors in [9] have proposed µSec-U (Microsec-U) Security Scheme for WSN. µSec is a link layer protocol for securing unicast communication for WSNs. The protocol supports basic security features such as confidentiality, integrity, authentication along with defending replay attack. µSec works on flat architecture of WSN in which the mode of communication between the nodes is unicast. A 128 bit key and a counter are pre-deployed into all nodes. The key is used for encryption/decryption of the message and the counter value is used to detect replay attack. µSec-U uses lightweight cryptographic algorithm which requires less computation overhead and less energy consumption.

In [10] the authors have proposed a Two Factor User Authentication Protocol (TFUAP) for WSNs. WSNs are deployed in a confined area. Authorized user can access WSN. For that first, user has to register with the gateway node of the network. Upon successful registration gateway node provides smart card to the user. With the help of smart card and password user can login to the gateway/sensor node and access data from the network. The protocol has two phases: Registration phase and Authentication phase. By registration phase user registers itself with a gateway node and obtains a personalized smart card. When user want to access the network, first he is authenticated by using password with smart card and then he is allowed to access the network. The gateway node does not maintain password/verifier table. For this reason the protocol resist from stolen verifier attack, and Guessing attack. The protocol also protects from Replay attack. Smart card is needed throughout the login session. The login session will be terminated upon removal of the smart card.

The authors in [11] have proposed SET-IBS and SET-IBOOS protocols for WSN. SET-IBS (Secure and Efficient data Transmission using the Identity Based digital Signature)and SET-IBOOS (Secure and Efficient data Transmission using the Identity Based Online-Offline digital Signature) are the protocols for clustered WSNs. Authentication of the encrypted sensed data is the key idea of both protocols. Digital signature is provided to message packets for authentication. The orphan node problem in a symmetric keymanagement is solved by these two protocols. Both protocol use ID – based cryptography with asymmetric key where ID information is a public key. User can obtain the corresponding private key without auxiliary data transmission. Thus energy is saved. Computation overhead of SET-IBS is reduced by using SET-IBOOS protocol.

In [12] the authors have proposed A Lightweight Hybrid Security Framework for WSN (LHSFW). In this framework the advantages of Intrusion Detection System (IDS) and Cryptography techniques are combined. Symmetric key cryptography is used in this framework. IDS detects internal and external attacks accurately, while cryptography techniques provide data confidentiality. The hybrid security framework provides privacy of communication and detects various attacks such as spoofed, altered or replayed routing information, man- in-the-middle and denial of service attacks. If we combine two techniques at each node then computation overhead and energy consumption is more. To solve this problem cryptography operations are applied during a certain mathematically determined period and only on those clusters where malicious node is detected. IDS removes almost all passive attacks by using cryptography techniques.

A Lightweight Secure Data Aggregation Technique (LSDAT) for WSN is proposed in [13]. In clustered WSN all nodes do not transmit data individually to the base station, but nodes within cluster send data to the CH/aggregator and then aggregator transmits data to the BS/sink. Thus the lifetime of the individual sensor is increased. But the problem is the aggregator exposes data in clear text and the data is vulnerable to various attacks by intruders. There are various techniques for solving this problem, but these techniques consider static node WSN. Nodes in the WSN may be dynamic. A lightweight secure data aggregation technique provides the solution for dynamic node WSN based on a cryptographic approach. The technique uses identity based encryption and pairing based cryptography. In this technique nodes establish shared secret key with their neighbours and thus provides encrypted data to the aggregator. This technique protects from Sybil attack, replay attack, wormhole attack and masquerade attack.

In [14] A Simple Lightweight Encryption Scheme (SLES) for WSN is proposed. This scheme provides an energy efficient lightweight encryption based on pseudorandom bit sequence. The bit sequence is generated by using elliptic curve cryptography. The scheme uses different base points of an elliptic curve to generate different pseudorandom bit sequence for two communication nodes. In this scheme first the key is established, than the pseudorandom bit sequence is generated and after that encryption is performed. In the encryption procedure first the plain text is converted to binary stream. Then the stream is xor-ed with the pseudorandom bit sequence and thus cipher text is generated. The XOR operation is used because when the key-stream is random, the additive cipher is more secure. The scheme can generate large bit sequence and that is why it is suitable for encryption of large volume of data such as image, audio and video.

A Lightweight Authentication Scheme (LAS) for WSN is proposed in [15]. This scheme composed of a key management and an authentication protocol. It uses symmetric key cryptography, unkeyed and keyed-hash functions. The main goal of the scheme is to provide confidentiality and authenticity. The protocol keeps minimum size and minimum number of interchanged messages. It is also capable to transport session keys. The main objective of the scheme is to provide energy efficiency. The scheme protects from resource consumption attack, and node capture attack and most danger denial of service attack. The memory requirement is small. The scheme depends on the number of neighbour nodes, and not on the total number of nodes in the network.

TABLE 1:Lightweight Security Mechanisms Analysis based on Security Goals

Security Mechanism	Authentication	Confidentiality	Integrity	Freshness
SQPS	✓		✓	✓
MSQPS		✓	✓	
SQPS_DT	✓		✓	✓
LOCHA	✓			
µSec-U	✓	✓	✓	
TFUAP	✓			
SET-IBS and SET-IBOOS	✓			
LHSFW		✓		
SLES		✓		
LAS	✓	✓		

TABLE 2:Lightweight Security Mechanisms Analysis based on Prevention of SECURITY ATTACKS

Security Mechanism	Differential Attack	Linear Attack	Replay Attack	Insider Attack
SQPS			✓	
MSQPS			✓	
SQPS_DT			✓	
µSec-U			✓	
SET-IBS and SET-IBOOS				
LHSFW			✓	
HIGHT	✓	✓		
BSPN	✓	✓		
TFUAP			✓	
LSDAT			✓	

IV CONCLUSION

In this paper, various lightweight cryptographic algorithms used to achieve different security mechanisms for WSN are surveyed. From the study, it can be concluded that, these various approaches [2, 3, 4, 6, 9, 10, 11. 12, 13, 14, 15] satisfy security goals viz. authentication, confidentiality, integrity, data freshness etc. Among the algorithms studied, we found that they are applied on application layer and provide security against replay attack, differential attack, linear attack etc. [2, 3, 4, 7, 8, 9, 10, 12, 13]. Simulation results of the various algorithm studied show that the proposed algorithms perform well and provide intended security. The informationprovided in this paper would be beneficial for the researchers to work in this area.

REFERENCES

[1] Sakthidharan, G. R., and S. Chitra. "A survey on wireless sensor network: An application perspective." In Computer Communication and Informatics (ICCCI), 2012 International Conference on, pp. 1-5, IEEE, 2012.

[2] Ghosal, Amrita, SubirHalder, Sanjib Sur, Avishek Dan, and SipraDasBit. "Ensuring basic security and preventing replay attack

in a query processing application domain in WSN." In Computational Science and Its Applications–ICCSA 2010, pp. 321-335, Springer Berlin Heidelberg, 2010,

[3] Ghosal, Amrita, and SipraDasBit. "A lightweight security scheme for query processing in clustered wireless sensor networks." Computers & Electrical Engineering 41,pp. 240-255, 2015.

[4] Ghosal, Amrita, SubirHalder, and SipraDasBit. "A dynamic TDMA based scheme for securing query processing in WSN." Wireless Networks 18, no. 2, pp.165-184, 2012.

[5] Sharma, Suraj, and Sanjay Kumar Jena. "A survey on secure hierarchical routing protocols in wireless sensor networks." In Proceedings of the 2011 International Conference on Communication, Computing & Security, pp. 146-151, ACM, 2011.

[6] Chowdhury, Amrita Roy, Tanusree Chatterjee, and SipraDasBit. "LOCHA: A light- weight one-way cryptographic hash algorithm for wireless sensor network." Procedia Computer Science 32, pp. 497-504, 2014.

[7] Koo, Woo Kwon, Hwaseong Lee, Yong Ho Kim, and Dong Hoon Lee. "Implementation and analysis of new lightweight cryptographic algorithm suitable for wireless sensor networks." In Information Security and Assurance, 2008. ISA 2008. International Conference on, pp.73-76, IEEE, 2008.

[8] Zhang, Xueying, Howard M. Heys, and Cheng Li. "Energy efficiency of symmetric key cryptographic algorithms in wireless sensor networks." In Communications (QBSC), 2010 25th Biennial Symposium on, pp. 168-172,IEEE, 2010.

[9] Ghosal, Amrita, Sanjib Sur, and SipraDasBit. "µSec: a security protocol for unicast communication in wireless sensor networks." In Proceeding of the SETOP international workshop on autonomous and spontaneous security, LNCS-7731,pp. 258-73, 2013.

[10] Das, ManikLal. "Two-factor user authentication in wireless sensor networks." Wireless Communications, pp. 1086-1090, IEEE Transactions on 8, no. 3, 2009.

[11] Lu, Huang, Jie Li, and Mohsen Guizani. "Secure and efficient data transmission for cluster-based wireless sensor networks." Parallel and Distributed Systems,pp. 750-761, IEEE Transactions on 25, no. 3, 2014.

[12] Sedjelmaci, Hichem, and Sidi Mohammed Senouci. "A lightweight hybrid security framework for wireless sensor networks." In Communications (ICC), 2014 IEEE International Conference on,, pp. 3636-3641,IEEE, 2014.

[13] MdMizanur Rahman, Sk, Mohammad Anwar Hossain, Maqsood Mahmud, Muhammad Imran Chaudry, Ahmad Almogren, Mohammed Alnuem, and AtifAlamri. "A lightweight Secure Data Aggregation Technique for Wireless Sensor Network." In Multimedia (ISM), 2014 IEEE International Symposium on, pp. 387-392, IEEE, 2014.

[14] Biswas, Kamanashis, VallipuramMuthukkumarasamy, ElankayerSithirasenan, and Kalvinder Singh. "A simple lightweight encryption scheme for wireless sensor networks." In Distributed computing and networking,, pp. 499-504, Springer Berlin Heidelberg, 2014.

[15] Delgado-Mohatar, Oscar, AmparoFúster-Sabater, and José M. Sierra. "A light-weight authentication scheme for wireless sensor networks." Ad Hoc Networks 9, pp.727-735, no. 5 , 2011.

[16] Hao, Dong, AvishekAdhikari, and Kouichi Sakurai. "Mixed-Strategy game based trust management for clustered wireless sensor networks." In Trusted Systems, pp. 239-257, Springer Berlin Heidelberg, 2012.

[17] Gu, Lize, Yun Pan, Mianxiong Dong, and Kaoru Ota. "Noncommutative lightweight signcryption for wirelesssensornetworks."International Journal of Distributed Sensor Networks, pp. 1-11,