A Survey on Cryptographic Schemes Used In Wireless Sensor Networks for Securing Communication

GunjanShrivastava[1], Prof. SandeepPratap Singh [2], Prof. Sanjay Sharma[3]

[1]M-Tech Research Scholar,[2]Asst. Prof, [3]HOD [1,2,3]Department of Computer science & Engineering, OIST, Bhopal

Abstract-The wireless sensor network is one of the most popular network technologies for different applications. A number of applications such as weather monitoring and geo-location tracking are implemented using the WSN technology. Because of which these networks are utilized in critical situations. Therefore the security in the communicated data is a primary aspect of the network for smooth functioning of the network. This paper provides the background of wireless sensor network. In this survey work, various techniques of cryptographic schemes for providing security in wireless sensor network are reviewed.

1. INTRODUCTION

Wireless Sensor Network basically consist of numerous sensors nodes and the wireless channel to connect the nodes and each node mainly consists of trans-receiver section, ultra-low power digital signal processor or microcontroller/microprocessor, external memory , various interfaces for data collection and power section. Number of nodes in any network varies from hundreds to thousands which makes it different than other wireless networks and therefore WSN is complex and challenging to control and maintain on continuous basis. As data is moving from various sensor nodes in the network the issues related to sensor data collection, data formatting, data transfer, data speed, data security and privacy, power optimization and power management, memory space and computational limitations, time delay and synchronization of the complete process and other related aspects opens new fields of research [1].

Wireless Sensor Network works in environment conditions especially where wired connections are not possible. Wireless sensor nodes consists of different types of sensors such as magnetic, thermal, visual, seismic, infrared and radar, which are able to monitor a wide variety of physical and environmental conditions.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Wireless sensor nodes contain array of sensors in case of multiple data collection. The sensor node can be put for continuous or selective sensing, location sensing, motion sensing and event detection etc. A base station links the sensor network to sense, process and disseminate information of targeted physical environments.

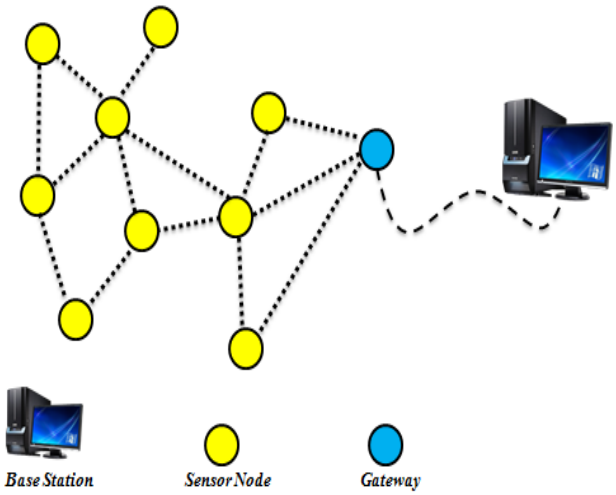

Figure 1 a typical View of WSN [1]

Wireless Sensor Networks Applications.

According to nature of Wireless Sensor Networks we can categorize the applications of WSNs into Defence applications, forest applications, medical science applications, Domestic applications, and industrial applications, etc.:

A. *Defence Applications:* WSNs can be an integral part of defence command, security control, data communications, computation, intelligence, targeting systems such as (C4ISRT), surveillance, reconnaissance etc.
B. *Forest Applications:* Some environmental applications of sensor networks include tracking and recording the movements of small animals ,birds and insects, monitoring environmental conditions, earth monitoring and exploration,
C. *Medical Science Applications:* Some of the health applications for sensor networks are diagnosing the patients, tracking location and movement of patients and doctors inside hospital etc.
D. *Industrial Applications:* Some industrial applications of WSNs are building virtual keyboards, monitoring

product quality, environmental control in office buildings, robot control, interactive toys etc.

Wireless Sensor Networks Challenges

A. Reliability: WSNs are wireless networks and are therefore vulnerable to problems like packet loss. Nevertheless, they are used in areas such as Chemical attack, detection, in which these Problems could easily lead to serious catastrophes.

*B. Power Consumption:*The nodes of Wireless Sensor Networks are usuallybattery powered because of their size. This limitsthe lifetime of a sensor node and raises the topic of energy- Efficiency in all aspects.

C.Node size: Miniaturization is the keyword in many studies about WSNs. Developing smaller nodes, with the same or even more efficiency than their bigger brothers is still a challenge, even if present sensor nodes, are hardly as big as a coin.

D. Mobility: Many applications urge the factor Mobility into WSN challenges. For example, commercial applications, like vehicle tracking, need networks that are able to constantly change its routing paths and infrastructure.

F. Privacy and Security: Unlike wired channels, wireless channels are accessible to both, legitimate and illegitimate users. Therefore, several methods, like encoding the traffic, have to be discussed.

Security Requirements

Wireless sensor networks are quite different from other wireless and wired networks. Security is very important in wireless communication as sensor nodes are deployed in real environment so easily vulnerable to different types of attacks and threats. For critical wireless sensor application security is main focus due to in real environment deployments of nodes, hacker attack the sensory nodes and will get the access to the data or may change the real data with false data/wrong information to the base station for false analysis of environment data. The security services should protect the information communicated over network and to protect sensor nodes from physical attacks or internal attacks [2]. Sensor networks are the key to gathering the information needed by smart environments, whether in buildings, utilities, industrial, home, shipboard, transportation systems automation, or elsewhere. Recent terrorist and guerilla warfare countermeasures require distributed networks of sensors that can be deployed using, e.g. aircraft, and have self-organizing capabilities. In such applications, running wires or cabling is usually impractical. A sensor network is required that is fast and easy to install and maintain [3].

2. BACKGROUND

Wireless sensor networks are vulnerable to various attacks like on nodes, network and on sensed data also. This section explains various types of attacks on sensor network.

Black-hole Attack

All packets are dropped by sending forged routing packets, the attacker could route all packets for some destination to itself and then discard them, or the attacker could cause the route at all nodes in an area of the network to point “into” that area when in fact the destination is outside the area[6]. In a black hole attack also known as packet drop attack, a malicious node insert a fake route replies to the route requests it obtain advertising itself as having the direct path to a destination.

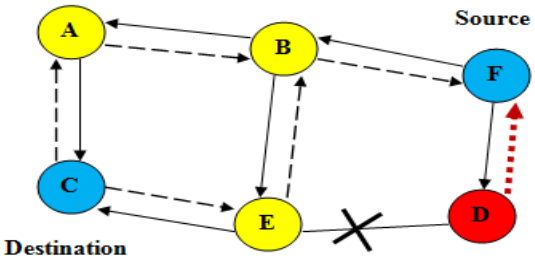

Figure 2 Black hole Attack

In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. An attacker intrudes communications originated by the sender, copies a portion or a whole packet, and speeds up sending the copied packet through a specific wormhole tunnel in such a way that the copied packet arrives at the

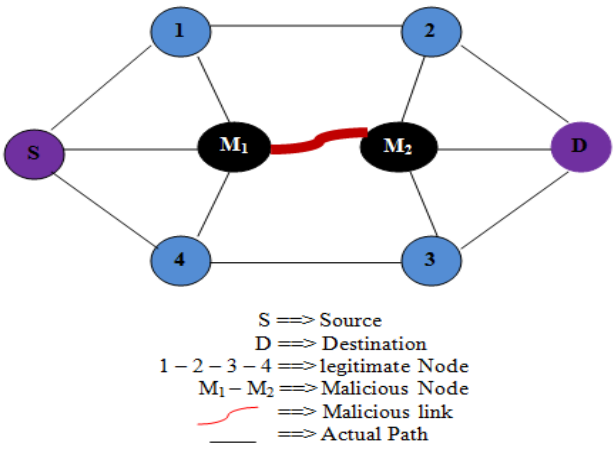

Figure 3Wormhole Attack

destination before the original packet which traverses through the usual routes. Such a tunnel can be created by several means, such as by sending the copied packet

through a wired network and at the end of the tunnel transmitting over a wireless channel, using a boosting long-distance antenna, sending through a low latency route, or using any out-of bound channel [7].

Sinkhole Attack

The sinkhole attack is a particularly severe attack that prevents the base station from obtaining complete and correct sensing data, thus forming a serious threat to higher-layer applications. In a Sinkhole attack [8], a compromised node tries to draw all or as much traffic as possible from a particular area, by making it look attractive to the surrounding nodes with respect to the routing metric.

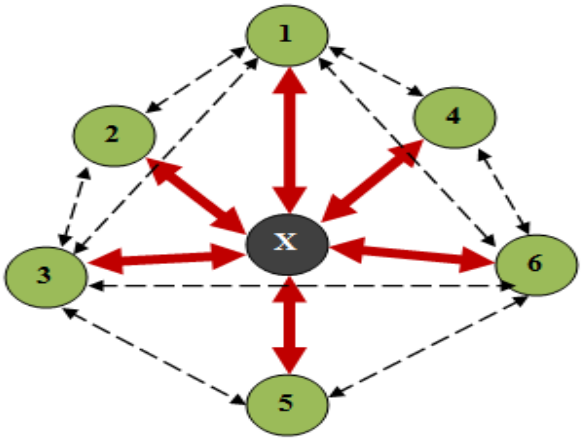

Figure 4 Sinkhole Attack

Sybil Attack

A single node presents itself to other nodes with multiple spoofed identifications (either MAC or network addresses). The attacker can impersonate other nodes identities or simply create multiple arbitrary identities in the MAC and/or network layer. Then the attack poses threats to other protocol layers; for examples, packets traversed on a route consisting of fake identities are selectively dropped or modified; or a threshold-based signature mechanism that relies on a specified number of nodes is corrupted [9].

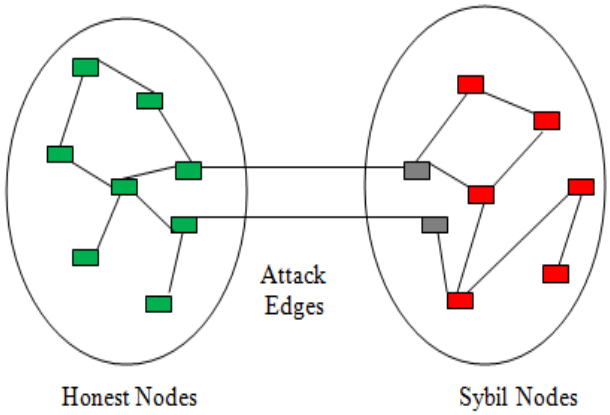

Figure 5 Sybil Attack

Cryptography

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as plaintext. It is encrypted into cipher text, which will in turn (usually) be decrypted into usable plaintext [9].

3. LITERATURE SURVEY

This section provides the study of the recently developed approaches for securing wireless sensor network of DNA based cryptography. The study of these techniques provides the guidelines for performance improvements of the traditional technique.

Security is one of the most significant and fundamental issue for data transmission in WSNs. Here in this paper MONIKA at el [12], the DNA concept for encryption with SSL protocol is used, which gives us three levels of security in WSN. In our proposed system the energy consumption problem for generating key pairs & generating certificates for sensor nodes are resolved to some extent by assigning key pairs & digital certificate before deploying sensor nodes in any environment. The public key & digital certificate sharing is done using the secure channel (SSL). Thus the computation overhead for sensor nodes for generating the keys may be reduced which may in turn reduce the computation time leading to energy efficiency in sensor nodes.DNA cryptography plays a vital role in areas of communications and data transmission. In DNA cryptography, biological DNA concept can be used not only to store data and information carrier, but also to perform computations. Monika et al [12] proposed a DNA based security. That uses DNA cryptography with secure socket layer (SSL) for providing a secure channel with more secure exchange of information in wireless sensor networks.

The objective of energy efficient routing protocol is to increase the operational lifetime of the wireless sensor networks. Multipath routing protocols enhance the lifetime of the wireless sensor networks by distributing traffic among multiple paths instead of a single optimal path. Transmission of secured data is also an important research concern in the wireless sensor networks. In this paper Shiva Murthy G et al [13] present, a secure node disjoint multipath routing protocol for wireless sensor networks is proposed. Here, the data packets are transmitted in a secure manner by using the digital signature crypto system. It is compared with an ad hoc on-

demand multipath distance vector routing protocol. It shows better results in terms of packet delivery fraction, energy consumption, and end-to-end delay compared to the ad hoc on-demand multipath distance vector routing. The given technique enhances the energy consumption in the network but the technique is not secured for data transmission. The proposed protocol provides the security using digital signature, which is generated by using the MD5 hash function and RSA algorithm. The security ensures the correctness of data, nonrepudiation and authentication. The proposed protocol defends data tampered or altered routing, selective forwarding, sink hole and byzantine attacks. In this paper EENDMRP is limited to physical data routing and multimedia data routing is not taken into consideration. A new metric measuring energy and QoS with link reliability is yet to be designed.

In a node replication attack, an adversary creates replicas of captured sensor nodes in an attempt to control information that is reaching the base station or, more generally, compromise the functionality of the network. In this work, Tassos Dimitriou [14] develop fully distributed and completely decentralized schemes to detect and evict multiple imposters in mobile wireless sensor networks (MWSNs). The proposed schemes not only quarantine these malicious nodes but also withstand collusion against collaborating imposters trying to blacklist legitimate nodes of the network. Contrary to prior work, the proposed schemes can effectively detect and quarantine the presence of *multiple* imposters faking the identity of *different* legitimate nodes in the network. We have proved the completeness and soundness Hence the completeness and soundness of the protocols are guaranteed. Our protocols are coupled with extensive mathematical and experimental results, proving the viability of our proposals, thus making them fit for realistic mobile sensor network deployments.

The wireless sensor networks continue to grow and become widely used in many applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, etc. There are many ways to provide security, one is cryptography. Selecting the appropriate cryptography method for sensor nodes is fundamental to provide security services in WSNs. Public Key based cryptographic schemes were introduced to remove the drawbacks of symmetric based approaches. Here Madhumita et al [15] compared two schemes in this paper ECC, and RSA and found out that ECC is more advantageous compared to RSA,due to low memory usage ,low CPU consumption and shorter key size compared to RSA. ECC have a significant advantage over RSA as it reduces the computation time and also the amount of data transmitted and stored. ECC 160 bits is two times better than RSA 1024 bits when code size and power consumption are the factors of consideration. Tests were performed in 8051 and AVR platforms as in[25].ECC 160 bits use four times less energy than RSA 1024 bits in Mica2dot as in[26].Recently a new scheme called Multivariate Quadratic Almost Group was proposed which showed significant improvements over RSA and ECC.

Security in wireless sensor network (WSN) is concern for a sensor networks and level of security desired may differ according to application specific needs where sensor networks are deployed. Most of the security techniques are used in WSN. The sensor node (SN) is used to collecting the information from the environment so it is necessary to secure our environment. There are many types of security provide in the field of WSN. Here KATIYAR at el. [16] take two technologies RSA algorithm and Biometrics techniques for the authentication in WSN and they are very effective to securing the information and message security by cryptographic technique and give the best result for authentication in WSN. These technologies are use to verifying the conformation of every single sensor node. In the study of RSA algorithm and Biometrics techniques the main features that both are in cryptography based and using the purpose for authentication security. In wireless sensor network these technologies are secure and give the efficient results, sometime during the research RSA is better than Biometrics for cost and more reliable changing security keys and Biometrics is use for the hard and strong security. In the bases of performance and popularity they both are lightly similar, but they are useful in WSN authentication security.

In this paper,Jiliang Zhou at el [17]propose efficient and secure routing protocol based on encryption and authentication for WSNs:BEARP, which consists of three phases: neighbor discovery phase, routing discovery phase, and routing maintenance phase. BEARP encrypts all communication packets and authenticates the source nodes and the base station (BS), and it ensures the four security features including routing information confidentiality, authentication, integrity, and freshness. Furthermore, we still design routing path selection system, intrusion detection system, and the multiple-threaded process mechanism for BEARP.Thus, all the secure mechanisms are united together to effectively resist some typical attacks including selective forwarding attack, wormhole attacks, sinkhole attacks, and even a node captured. Our BEARP especially mitigates the loads of sensor nodes by transferring routing related tasks to BS, which not only maintains network wide energy equivalence and prolongs network lifetime but also improves our security mechanism performed uniquely by the secure BS. Simulation results show a favorable increase in performance for BEARP when compared with directed diffusion protocol and secure

directed diffusion protocol in the presence of compromised nodes.

In the paper, AMIT KUMAR SINGH[18] have proposed a security architecture that provides confidentiality, integrity, and authentication for a mobile wireless sensor network. Based on the Boneh-Franklin IBE algorithms, he proposed an identity-based key distribution and encryption scheme for wireless sensor networks. Analysis shows that our scheme has some advantages in terms of key management, storage requirement and security. The large number of new applications for wireless sensor networks has lead to unprecedented growth of wireless sensor networks. For this purpose, he have presented algorithms to easily setup pair wise secret keys between the mobile sensor nodes and to establish identity based secret key per node, in which it can communicate its messages securely. Furthermore, our solution minimizes the effects of compromised nodes. Compromising an adjustable number of sensor nodes does not compromise the whole security architecture but restricts the security breach to the immediate neighborhood of the compromised node. Finally, we have implemented a prototype of our security architecture, which clearly shows that it is a lightweight solution and applicable for self-organizing mobile wireless sensor networks.

Secure data transmission is a critical issue for wireless sensor networks (WSNs). Clustering is an effective and practical way to enhance the system performance of WSNs. In this paper, we study a secure data transmission for cluster-based WSNs (CWSNs), where the clusters are formed dynamically and periodically. In this paper HUANG LUat el[19]propose two secure and efficient data transmission (SET) protocols for CWSNs, called SET-IBS and SET-IBOOS, by using the identity-based digital signature (IBS) scheme and the identity-based online/offline digital signature (IBOOS) scheme, respectively. In SET-IBS, security relies on the hardness of the Diffie-Hellman problem in the pairing domain. SET-IBOOS further reduces the computational overhead for protocol security, which is crucial for WSNs, while itssecurity relies on the hardness of the discrete logarithm problem. In the evaluation section, we provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SETIBOOS are efficient in communication and applying the ID based cryptosystem, which achieves security requirements in CWSNs, as well as solved the orphan node problem in the secure transmission protocols with the symmetric key management. We show the feasibility of the SET-IBS and SET-IBOOS protocols with respect to the security requirements and security analysis against various attacks. The calculations and simulations are provided to illustrate the efficiency of the proposed protocols. The results show that the proposed protocols have better performance than the existing secure protocols for CWSNs, in terms of security overhead and energy consumption.

4. CONCLUSION

The wireless sensor networks continue to grow and become widely used in many applications. So, the need for security becomes vital. However, the wireless sensor network suffers from many constraints such as limited energy, processing capability, and storage capacity, etc. There are many ways to provide security, one is cryptography. Selecting the appropriate cryptography method for sensor nodes is fundamental to provide security services in WSNs. In this paper the cryptographic techniques and their applications for securing wireless sensor network are discussed. We have gone through wireless sensor network applications and security issues and threats in wireless sensor network. In addition of that how traditional cryptography is replaced by new generation cryptographic algorithms are also studied. It is an important challenge to find out suitable cryptography for wireless sensor networks due to limitations of power, computation capability and storage resources. In this review article we have analyzed about the different techniques of the cryptography for providing the security in the wireless sensor network.

REFERENCES

[1] Anjali Potnis1, and C S Rajeshwari, “Wireless Sensor Network: Challenges, Issues and Research”, *Proceedings of 2015 International Conference on Future Computational Technologies (ICFCT'2015)*, pp. 224-228, March 29-30, Singapore, 2015.

[2] Lovepreetkaur and JyoteeshMalhotra, “Review on Security Issues and Attacks in Wireless Sensor Networks”, *International Journal of Future Generation Communication and Networking*, PP. 81-88, Vol. 8, No. 4 (2015).

[3] F. L. LEWIS, “Wireless Sensor Networks”, *to appear in Smart Environments: Technologies, Protocols, and Applications*, New York, 2004.

[4] PardeepKaur and VinayBhardwaj, “Wireless Sensor Networks: A Survey”, *International Journal of Advanced Research in Computer Science and Software Engineering*, PP. 988 – 994, Volume 5, Issue 5, May 2015.

[5] Jennifer Yick andDipakGhosal, “Wireless Sensor Network Survey”, Computer Networks, Volume 58, PP. 2292-2330, April 2008.

[6] N.Saravanan, K.Pazhanisamy, “A Survey – Secure Routing in Mobile Ad hoc network”, *International Research Journal of Latest Trends in Engineering and Technology (IRJLTET)*, Vol. 1, Nov/Dec 2014, PP. 1-6.

[7] K.Venkatraman and J. Vijay Daniel, "Various Attacks in Wireless Sensor Network: Survey", *International Journal of Soft Computing and Engineering (IJSCE)*, Volume-3, Issue-1, March 2013.

[8] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", *International Journal of Engineering and Advanced Technology (IJEAT)*, Volume-1, pp. 269-275, June 2012.

[9] M.Kundalakesi, Sharmathi.R and Akshaya.R, "Overview of Modern Cryptography", *International Journal of Computer Science and Information Technologies (IJCSIT)*, Volume 6, PP. 350-353, 2015.

[10] Pierluigi Paganini, ―The Future of Data Security: DNA Cryptography and Cryptosystems‖, February 20, 2015.

[11] RadhaShinde and LalitGehlod, "A Survey on DNA Based cryptography", *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, Volume 5 Issue 1, January 2016.

[12] Monika a*, ShuchitaUpadhyaya , Secure communication using DNA cryptography with secure socket, 4thInternational Conference on Eco-friendly Computing and Communication Systems, layer (SSL) protocol in wireless sensor networks,(2015) Elsevier.

[13] Shiva Murthy G, Robert John D' Souza, and GollaVaraprasad, "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks", IEEE SENSORS JOURNAL, VOL. 12, NO. 10, OCTOBER 2012.

[14] TassosDimitriou, Ebrahim A. Alrashed, MehmeHakankarata and Ali Hamdan, "Imposter Detection for Replication of Attacks in Mobile Wireless Sensor Networks", 7th International Confrence on New Technologies, Mobility and Security (NTMS), 2015 IEEE.

[15] Madhumita Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques" American Journal of Engineering Research (AJER)

[16] Sandhyakatyar,shumailarizwanand DR. rajnish Gujral"Network Security Described Technology Based on RSA and Biometrics for Authenticity in WSN" International Journal of Advanced Research in Computer Science and Software Engineering, vol 6, issue 2, feb 2016.

[17] JiliangJhou,"Efficient and Secure RountingProtocol based on Encryption and Authentication for Wireless Sensor Networks", Hindawai Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013 Article ID 108968, 17 pages.

[18] AmitKumar Singh "Identity-Based Key Distribution for WirelessSensor Networks using Cryptographic Techniques" International Journal on Emerging Technologies 2015.

[19] HuangLu,Jie Li and Mohsen Guizani" Secure and EfficientDataTransmissionfor Cluster-Based Wireless Sensor Networks" IEEE Transactionson ParallelAnd Distributed Systems, Vol. 25, No. 3, March2014.