Detection Techniques for Selective Forwarding Attack in Wireless Sensor Networks

Surinder Singh, Hardeep Singh Saini

Abstract--- A Wireless Sensor Network (WSN) consist of sensing area, base station, internet and user which can measure and predict temperature, sound, wave, vibration, pressure etc. As the transmission of data is involved in WSN and Transmission Control Protocol/Internet Protocol (TCP/IP) is used for sending the data to the base station. The security of transmitting the data is crucial as the data contain precious information. The attacker can attack any layer of TCP/IP protocol. The network layer may prone to selective packet dropping attack, Sybil attack, Wormhole attack, Black-hole attack and Denial of Service (DOS) attack. These kinds of attacks can be overcome by using key management process. The communications between the nodes are only possible through these keys. The security of data transmission can be increased by using key environment in wireless sensor network. The number of detection techniques based on Key management process is discussed in this paper. These techniques are Public Key Encryption (PKE), Rivest Shamir Adelmen (RSA), ELGAMAL and Chinese Reminder Theorem (CRT) based RSA. In this paper, detailed study for these techniques on the basis of storage space required, energy consumption and time consumption for key exchange parameters has been discussed

Index Terms—Attacker node, Sensor node, Wireless sensor network.

I. INTRODUCTION

Recent advancement in Wireless Sensor Networks (WSNs) create a challenge for researchers to design a low cost, low power and secure sensor nodes [1]. A small sensor consists of sensing, data processing unit and transmission element to sense, process and transmit the data. A sensor has inbuilt processer which is capable to process the data and send only the required data to another sensor node. The data processing capability of sensor creates its application in health, military and other sensitive area of battlefield. To use wireless sensor network in different application the different routing and data aggregation protocols were developed [2][3][4]. The critical issue which focus the mind of researcher is security of sensed data. As a sensor node has a trans-receiver which is capable to transmit and received the wireless data. An attacker can easily generate a code to retrieve all the information from the sensor. A wireless sensor network consists of many sensor nodes for sensing various types of data within the network. These sensors may be connected in cluster or any other depending upon the application. A network which is prone the security threat from the attacker node need more security [5][6][7]. A security is more challenged when the network used in military or any defence application where zero tolerance required for securing of important data. An attacker can attack wireless sensors in many ways. Depending upon the code create by the attacker the attacks can be classified into many types. A widely used transmission protocol that is Transmission control Protocol/Internet

Protocol (TCP/IP) be capable to transmit or receive the data within the network. An Attacker can attack any layer of TCP/IP protocol and retrieve the important data from sensor node. Table 1 shows the layer wise possible attacks and their impacts.

Table 1. Layer wise possible attacks and their impacts

Layers	Attacks	Impact
Application Layer	SQL injection Attack	The security vulnerability within the database layer of an application layer is exploited using the SQL injection attack[8].
Transport Layer	Port Scan Attack	In order to explore the vulnerabilities of the system, the attacker finds the ports that are available using the port scan [9].
Network Layer	Selective packet dropping attack, Denial of Service attack Wormhole attack, Blackhole attack	A designing of a 3-way handshake which initiates a TCP connection holds the basis of SYN flooding attack. The ability of an initiator in the direction of get delivery of packet next to the IP address which was worn by it like spring within early request is verified by the third packet using this handshake [10].
Data-Link Layer	Media Access Control (MAC) Address spoofing	A known MAC address a part of another host is utilized for making mark toggle onward frame which are intended in support of distant swarm towards set of connections assailant through the MAC spoofing attacks [11].
Physical Layer	Someone knows how to bodily depart whole set-up card otherwise disconnect the internet wire.	Don't let people touch your computer[12].

Revised Manuscript Received on March 10, 2019.

Surinder Singh, Research Scholar, IKG PTU, Kapurthala, Punjab, India. (E-mail: sunny16387@gmail.com)

Hardeep Singh Saini, Professor, Indo Global College of Engineering, Abhipur, Punjab, India. (E-mail: hardeep_saini17@yahoo.co.in)

Out of all layers a network layer prone various types of attacks that is Selective packet dropping attack, Denial of Service attack, Wormhole attack and Blackhole attack. Selective forwarding attack is an interior type attacks. In this attack a malicious node (attacker node) is created [13][14][15]. This node sends few messages and drops others. Attacker tries to be following the actual path of data flow between the sensor nodes. In this attack malevolent vertex exists similar to usual vertex within the majority occasion other than particularly plummet receptive packet, that exposure a faction to opposite forces. Selective forwarding attack is tough toward discern, since packet drops inside sensor networks may be caused by unpredictable wireless communications or node failure. Fig 1 shows the selective packet dropping attack. The red nodes are the affected node which can attack by the attacker node. An attacker node enters into routing protocol and retrieves all important data from the sensors. In this attack the attacker drop the packets by routing these packets towards attacker node. The black nodes are the attacker/Malicious nodes in fig 1.The white circles are not affected sensor nodes. The green circle is the base station where all important data can be transferred from sensor nodes within the network. The base station is also prone to this attack. The base station has more backup than a normal sensor node. A heavy routing and data aggregation protocol can implement to increase the security base station. Security never wants free. Whenever more security highlights are brought into the system, in parallel with the improved security quality is the consistently expanding calculation, correspondence, and administration overhead. Subsequently, organize execution, as far as adaptability, benefit accessibility, strength, thus one of the security arrangements, turns into an essential worry in an asset obliged impromptu arrange. While numerous contemporary recommendations centre on the security life of their answers from the cryptographic point of view, they clear out the system execution angle generally unaddressed. Actually, the two measurements of security quality and system execution are similarly critical, and accomplishing a decent exchange off between two extremes is one basic test in security plan for WSN. The security in remote sensor systems (WSN) is a basic issue because of the natural constraints of computational limit, stockpiling limit and power utilization. Bundles are dropped or disposed of totally, or specifically sent by an unknown gathering. Additionally the system is overwhelmed with worldwide suspicious communicates. These sorts of assaults might be maintained a strategic distance from when utilizing multi way and confirmed communicates, which must be encouraged by the fundamental key administration engineering. Key administration just ensures the conveying hubs have the essential keys, in the meantime giving the secrecy, uprightness and credibility of the imparted information. remote sensor systems (WSNs) are progressively utilized as a part of numerous applications like propensity observing, social insurance, military or security territories Since sensor hubs frequently dwell in unattended or antagonistic condition, especially with military applications, an enemy could without much of a stretch access the remote channel and block the transmitted data, or appropriate false data in WSN. Under such conditions, confirmation and privacy ought to be experienced to guarantee honesty of sensor hub and legitimate usefulness of the system.

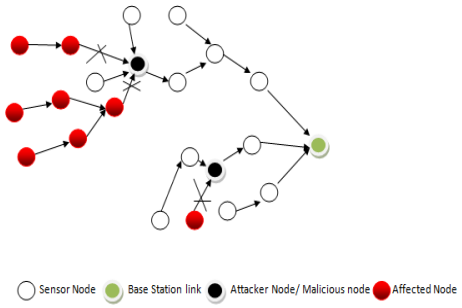

Fig. 1 Selective packet dropping attack

II. DETECTION TECHNIQUES

In this section, few detection schemes for selective packet dropping attack are discussed. These techniques are Public Key Encryption (PKE), Rivest Shamir Adelmen (RSA), ELGAMAL and Chinese Reminder Theorem (CRT) based RSA. The performance of above techniques can be calculated on the basis of Storage space required, Energy consumption and Time consumption for key exchange. The detail study for these techniques on the basis of above said parameters. Based on previous work the detection schemes are classified as

- Public Key Encryption (PKE) [9].
- Rivest Shamir Adelmen (RSA) [10].
- ELGAMAL Detection [11].
- Chinese Reminder Theorem (CRT) based RSA [12].

2.1 A Public Key Encryption (PKE)

It is symmetric cryptography technique used in military and domestic applications. In this method the message is transmitted with key management method. An encrypted key can only be decrypted if both are matched. The information security can be increased as only a authentic data can be transmitted within the wireless sensor network. As a secure algorithm is used to generate an encrypted key, the attacker cannot retrieve the important data from the sensor node. An example is taken to understand how the data get secured using this method. Suppose in wireless sensor network there are two sensor and base station A, B and C. The A sensor can send a data to B sensor and B sensor can send the data to the base station C. The data from the A sensor can be transmitted to B sensor through encrypted key algorithm. The B sensor can only receive the data if they have decrypted key algorithm. Similarly the B sensor can send to the base station through similar process. The security of data of data can be increased with this manner. The main advantage of this technique is that storage space requirement is less. The energy consumed by the sensor node to process this type of algorithm is less [16].

2.2 Rivest Shamir Adelmen (RSA)

This technique was invented by Ron Rivest, Adi Shamir and Len Adleman. The reason for this technique named as Rivest Shamir Adelmen (RSA). This method based on public and private key generation. The security of this method depends upon the RSA cryptosystem which is public key cryptosystem. In this method the data from the sender node can be converted into ciphertext and it can only be retrieved by the receiver node if they have the private key ciphertext. The main problem by which attacker cannot able to attack the sensor node that is to generate a private key is equivalent to factoring the modules key n. An attacker cannot detect the information until they modules key n. The main strength of this technique is that storage space requirement for public as well as private key would be less. Due to this energy consumed by the sensor node to process this type of algorithm is less and also the time consumption to exchange the public/private key would be less which affect the overall performance of the wireless sensor network [17].

2.3 ELGAMAL Detection

It was described by Taher Elagmal in 1985.This technique based on public key cryptography method. This is an asymmetric key encryption scheme in which the message can only be decoded using public/Private key. The receiver can only decode the data if the private key matched with public key. The encrypted message can only be decrypted with receiver private key. This type of method finds their application in information security. This detection scheme consists of three components that is Key generator, the encryption algorithm and decryption algorithm. The key generator generates the public/private key. The public key is kept with sender and private key kept with receiver. The use of public key can only be possible with encryption algorithm whereas the use of private key possible with decryption algorithm. The main drawback of this technique is that storage space requirement for public as well as private key would be high. Due to energy consumed by the sensor node to process this type of algorithm is more and also the time consumption to exchange the public/private key would be high which affect the overall performance of the wireless sensor network [18].

2.4 Chinese Reminder Theorem (CRT) based RSA.

RSA is more effective in Chinese Remainder Theorem mode than in direct mode. As it handles information with a large portion of the RSA modulus estimate, RSA with CRT is hypothetically around four times quicker and is in this way more qualified to remote sensor systems. In this view we proposed another effective key administration conspire RSA-CRT calculation to help both multi way and hub particular key pre-appropriation for verification of message communicate in Wireless Sensor Networks (WSNs). This strategy takes the benefits of the self implementing plan i.e. open key calculation and key pre circulation conspire and are joined together to accomplish productive key administration plot which will diminish the vitality utilization and correspondence overheads even with constrained assets. The main strength of this technique is that storage space requirement for public as well as private key would be less. Due to this energy consumed by the sensor node to process this type of algorithm is less and also the time consumption to exchange the public/private key would be less which affect the overall performance of the wireless sensor network The table 2 shows the comparison of all four techniques with respect to Storage space required, Energy consumption and Time consumption for key exchange [19].

Table 2. Comparison of detection schemes for selective packet dropping attack results

Sr.No	Parameter	ELGAMAL[9]		RSA[10]	
1.	Storage space required (in MB)	No. of nodes =20	0.30	No of nodes=20	0.20
2.	Energy consumption (in mW)	No. of nodes =200	1120	No of nodes =200	273.8
3.	Time consumption for key exchange	Key size (in bits)=160	3	Key size (in bits)=160	3

Sr.No	Parameter	PKE[11]		CRT based RSA[12]	
1.	Storage space required (in MB)	No. of nodes =20	0.10	No. of nodes =20	0.15
2.	Energy consumption (in mW)	No. of nodes =200	527.74	No. of nodes =200	126.32
3.	Time consumption for key exchange	Key size (in bits)=160	4	Key size (in bits)=160	3

III. CONCLUSION & FUTURE SCOPE

Security is a crirtical issue in wireless sensor network. The wireless sensor network prone to various types of attacks.Out of all these attacks the selective packet dropping is one of the major threat to wireless sensor network. To Overcome this attack a key managment enviorment can be used in the network. Based on this enviorment, four detetcion techniques are discussed in this paper. These technqiues are Public Key Encryption (PKE), Rivest Shamir Adelmen (RSA), ELGAMAL and Chinese Reminder Theorem (CRT) based RSA. The performance of above techniques can be calculated on the basis of storage space required, energy consumption and time consumption for key exchange. The Public Key Encryption requires minimum storage size. The CRT based RSA requires minimum Energy consumption and time consumption for key exchange. The Public Key Encryption and CRT based RSA can be used as hybrid approach to increase the overall network performance in terms of Storage space required, Energy consumption and Time consumption for key exchange.

REFERENCES

1. G. Sharma, S. Bala, and A. K. Verma, "Security Frameworks for Wireless Sensor Networks-Review," Procedia Technol., vol. 6, pp. 978–987, 2012.
2. P. Schaffer, K. Farkas, Á. Horváth, T. Holczer, and L. Buttyán, "Secure and reliable clustering in wireless sensor networks: A critical survey," Comput. Networks, vol. 56, no. 11, pp. 2726–2741, 2012.
3. Y. Yu, K. Li, W. Zhou, and P. Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures," J. Netw. Comput. Appl., vol. 35, no. 3, pp. 867–880, 2012.
4. M. Masdari, S. M. Bazarchi, and M. Bidaki, "Analysis of Secure LEACH-Based Clustering Protocols in Wireless Sensor Networks," J. Netw. Comput. Appl., vol. 36, no. 4, pp. 1243–1260, 2013.
5. M. A. Mahmood, W. K. G. Seah, and I. Welch, "Reliability in wireless sensor networks: A survey and challenges ahead," Comput. Networks, vol. 79, no. December, pp. 166–187, 2015.
6. B. Rashid and M. H. Rehmani, "Applications of wireless sensor networks for urban areas: A survey," J. Netw. Comput. Appl., vol. 60, pp. 192–219, 2016.
7. N. Rouissi and H. Gharsellaoui, "Improved Hybrid LEACH Based Approach for Preserving Secured Integrity in Wireless Sensor Networks," Procedia Comput. Sci., vol. 112, pp. 1429–1438, 2017.
8. C.-F. Wang, J.-D. Shih, B.-H. Pan, and T.-Y. Wu, "A Network Lifetime Enhancement Method for Sink Relocation and Its Analysis in Wireless Sensor Networks," IEEE Sens. J., vol. 14, no. 6, pp. 1932–1943, 2014.
9. X. Wu, H. Lin, and G. Li, "An improved routing algorithm based on LEACH protocol," Proc. - 9th Int. Symp. Distrib. Comput. Appl. to Business, Eng. Sci. DCABES 2010, pp. 259–262, 2010.
10. M. Nikodem and B. Wojciechowski, "Upper Bounds on Network Lifetime for Clustered Wireless Sensor Networks," 2011 4th IFIP Int. Conf. New Technol. Mobil. Secur., pp. 1–6, 2011.
11. H. Ochiai, H. Ishizuka, Y. Kawakami, and H. Esaki, "A Delay-Aware Data Collection Network Structure for Wireless Sensor Networks," IEEE Sens. J., vol. 11, no. 3, pp. 699–710, 2011.
12. Z. Wang, E. Bulut, and B. K. Szymanski, "Energy Efficient Collision Aware Multipath Routing for Wireless Sensor Networks," 2009 IEEE Int. Conf. Commun., pp. 1–5, 2009.
13. Mainwaring, A., Polastre, J., Szewczyk, R., Culler, D., Anderson, J.: Wireless SensorNetworks for Habitat Monitoring. In: First ACM Workshop on Wireless Sensor Networks and Applications, Atlanta, GA, USA (September 2002)
14. Fuchs, G., Truchat, S., Dressler, F.: Distributed Software Management in Sensor Networks using Profiling Techniques. In: 1st IEEE/ACM International Conference on Communication System Software and Middleware (IEEE COMSWARE 2006): 1stInternational Workshop on Software for Sensor Networks (SensorWare 2006), New Dehli, India (January 2006)
15. Zhang, W., Cao, G.: Group Rekeying for Filtering False Data in Sensor Networks: A Predistribution and Local Collaboration-Based Approach. In: 24th IEEE Annual Joint Conference of the IEEE
16. Yang, H., Luo, H., Ye, F., Lu, S., Zhang, L.: Security in mobile ad hoc networks: challenges and solutions. IEEE Wireless Communications 11(1), 38–47 (2004)
17. Delgosha, F.: Senier member of IEEE A multivibrate key establishment scheme for wireless sensor networks. IEEE Transaction on wireless communication 18 (April 2009)
18. Xiao, Y., Rayi, V., Sun, B., Du, X., Hue, F.: A survey of key management schemes in wireless sensor networks. Computer Communications 30, 2314–2341 (2007)
19. P. Kalyani and C. Chellappan,: Analysis of Security and Key Management Schemes for Authenticated Broadcast in Heterogeneous Wireless Sensor NetworksSpringer-Verlag Berlin Heidelberg 2011 pp. 580–587, 2011