International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

A Review on Security Concepts for Secure Multihop Routing Protocol

Garima[1], Sandeep Kumar[2]
[1]M. Tech scholar, ECE Department, Guru Nanak Institute of Technology, Haryana
[2]A. P., ECE Department, Guru Nanak Institute of Technology, Haryana

Abstract: **Wireless Sensor Networks (WSNs) are vulnerable to different kinds of attacks and most of traditional networks security techniques are unusable on WSNs; due to untrusted transmissions, deployment in open and hostile environments, unattended nature and limited resources. So, security is a vital and complex requirement for these networks. This paper focuses on security of WSNs and its main purpose is discussing on WSNs' attacks in different layers, including of physical layer attacks, link layer attacks, routing layer attacks, transport layer attacks and application layer attacks. It classifies and compares different attacks based on their nature and goals; i.e. this paper is expressing purpose and capabilities of attackers and it is presenting goals and result of different attacks on WSNs.**

Keywords: **- WSN, MRP, Attacks, Security**

I. INTRODUCTION

A wireless sensor network (WSN) (sometimes called a wireless sensor and actor network (WSAN)) are spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively supply their information through the connecting nodes to a particular position. Many modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial method displaying and handle, machine health displaying, and so on.

The WSN is developed of "nodes" – from some to many hundreds or even thousands, where each node is linked to one (or sometimes several) sensors. A radio transceiver with an internal antenna or link to an external antenna, a microcontroller, an integrated circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might change in size from that of a shoebox decrease to the size of a wheat grain, although performing "motes" of genuine microscopic boundaries have yet to be issued.

The process of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Price of constraints on sensor nodes is outcome in relating constraints on some parameters as like energy, memory, computational speed and communications bandwidth. The type of connecting network for the WSNs can change from a simple star network to an advanced multi-hop wireless mesh network. The propagation method between the hops of the connector can be transmitting or flooding.

II. MULTIPATH ROUTING PROTOCOL (MRP)

This is the routing method of using multiple alternative ways through connecting nodes, which can yield a variety of benefits such as fault tolerance, increased bandwidth, or improved security. The multiple paths calculated might be crossover, edge-dis-linked or node-dis-linked with each other. Main research has been done on multipath routing methods, but multipath routing is not yet widely deployed in practice. Constructive and destructive interference occurred due to effect of multipath, and phase position change of the signal. Destructive interference causes fading. Where the magnitudes of the signals rising by the different paths have a distribution known as the Rayleigh spread, this is known as Rayleigh fading. A part of device represents, a Rician spreading gives a more right model, and this is called as Rician fading.

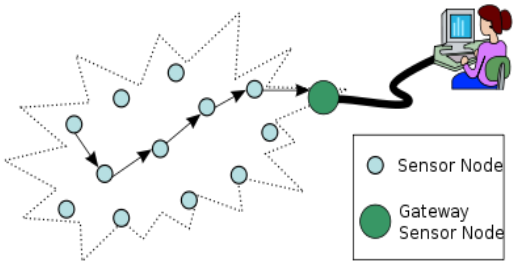

Figure 1: Typical multi-hop wireless sensor network architecture

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

III. LITRETURE SURVEY

This subsection explains and examines existing work on most general algorithm implementation for both software and hardware methods. The metrics taken into consideration are processing speed, throughput, power consumption, and packet size and data types.

When applied for wireless sensor networks. While in Asymmetric Encryption, two keys are used. The SCADA communication takes place over radio, modem, or devoted serial lines. The internet SCADA facility has brought several advantages in terms of control, data generation and presentation. With these advantages, come the security issues about web SCADA. Masadeh, Turab (2010) this paper encryption algorithm are compared on the basis of wireless network. Encryption methods play a hero role in wireless network security systems. However, these schemes consume a significant amount of computing resources such as CPU time, and packet size [9]. This can be extended too many rounds. They developed RSA encryption technique in a way to be performed in the general linear group on the ring of integer mod n. The encryption process has no foundation in encryption and decryption way and is claimed to be efficient, scalable and dynamic. To remedy the wireless network security issue, a novel work has been deployed to secure the transmitted data over wireless network and examine a method for analyzing trade-off between efficiency and security. A comparison has been conducted for those encryption techniques at different settings for each method such as different sizes of data blocks, different platforms and different encryption/decryption speed. They offered proof of concept by applying a definite privacy homomorphism for sensor network. Sorry to say as shown by Rivest, et al., any privacy homomorphism is unconfident even against cipher text that only attacks if they support comparison operations [10]. In this paper we show that a particular order preserving encryption technique achieve the above mentioned energy benefits and give when used to support comparison operations over encrypted texts for wireless sensor networks. The technique is shown to have reasonable memory and computation. In this paper, comparison between Encryption techniques as used in Communication between SCADA Components is discussed. The reason reverse to the efficiency (separate nodes perform different tasks), fault-tolerance (if some nodes are occupied then others can perform the task) and security (the trust essential to perform the task is shared between nodes) that order differently [11].

Evaluating the Effects of Cryptography Algorithms on power consumption for wireless devices has done by D. S. Abdul. Elminaam et.al, (2009) presents a performance evaluation of selected symmetric encryption algorithms on power consumption for wireless devices. Several points can be concluded from the Experimental results. First; in the case of changing packet size with and without transmission of data using different architectures and different WLANs protocols, it was concluded that Blowfish has better performance than other common encryption algorithms used, followed by RC6. Second; in case of changing data type such as audio and video files, it is found the result as the same as in text and document. In the case of image instead of text, it was found that RC2, RC6 and Blowfish has disadvantage over other algorithms in terms of time consumption. He is found that 3DES still has low performance compared to algorithm DES. Third point; [12] when the transmission of data is considered there was insignificant difference in performance of different symmetric key schemes (most of the resources are consumed for data transmission rather than computation). There is insignificant difference between open key authentications and shared key authentication in ad hoc Wireless LAN connection with excellent signals. In case of poor signal it is found that, transmission time increased minimum by 70 % over open sheered authentication in ad hoc mod. Finally -in the case of changing key size – it can be seen that higher key size leads to clear change in the battery and time consumption.

Comparison of Data Encryption Algorithms has done by Simar Preet Singh, and Raman Maini -The simulation results showed that Blowfish has better performance than other commonly used encryption algorithms. AES showed poor performance results compared to other algorithms, since it requires more processing power. The first sets of experiments were conducted using ECB Mode. The results show the superiority of Blowfish algorithm over other algorithms in terms of processing time. It shows also that AES consumes more resources when data block size is relatively big. Another point can be noticed here that 3DES requires always more time than DES because of its triple phase encryption characteristic. Blowfish, which has a long key (448 bit), outperformed other encryption algorithms. DES and 3DES are known to have worm holes in their security mechanism; Blowfish and AES do not have any so far [13].

As expected, CBC requires more processing time than ECB because of its key-chaining nature. The results indicate also that the extra time added is not significant for many applications, knowing that CBC is much better than ECB in terms of protection.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 7, Issue 7, July 2017)

Evaluation of Performance Characteristics of Cryptosystem Using Text Files designed by challa Narasimham and Jayaram Pradhan in 2008 they performed the performance comparison for variable sized text files as input. An analysis on computational running times results in significant difference among the methods. He believe in that the performance of DES, especially in decryption method is very high than the alternatives. Despite the key distribution, DES is more suitable to the application, which has the decryption as the highest priority. He has proposed and performed the test cases on the two PKCS methods i.e., RSA and NTRU Though the encryption, decryption and complexity are high in NTRU, the RSA provides the highest security to the business application. He presented all these parameters with computational running times for all the methods, so as to select the appropriate method [14].

Abdel-Karim and his colleague Al Tamimi presented simulation results showed that Blowfish has a better performance than other common encryption algorithms used. Since Blowfish has not any known security weak points so far, which makes it an excellent candidate to be considered as a standard encryption algorithm? AES showed poor performance results compared to other algorithms since it requires more processing power. Using CBC mode has added extra processing time, but overall it was relatively negligible especially for certain application that requires more secure encryption to a relatively large data blocks.

The results showed that Blowfish has a very good performance compared to other algorithms. Also it showed that AES has a better performance than 3DES and DES. Amazingly it shows also that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data [15].

IV. Problem Statement

The sensor networks can be deployed in a hostile environment for handling sensitive information. These networks may be prone to many attacks by the adversary for data capturing, creating malicious nodes, etc. There are number of attacks which can be performed during the transmission of data from source node to destination node like, packet drop attack, Black hole attack, Sybil attack, wormhole attack, hello flooding etc. These sensor nodes are also resource constraint.

Packet drop attack: The nodes in an ad hoc network communicate using wireless links which are by nature vulnerable to interference and channel errors that may corrupt some or many data packets.

Moreover, the nodes share the physical medium, compete to transmit data packets and suffer collisions. Thus, one of the problems in detecting malicious nodes that drop packets is that it may not be clear as to whether the packet was dropped due to channel errors, collisions, or due to malicious intent. In most detection mechanisms, the number of packets that are not forwarded is recorded by a passive listener. A threshold on the number of dropped packets is then used to decide whether or not a node is malicious. Depending on the threshold and data load, a burst of errors on the channel or an increase in the number of collisions can trip the threshold creating false alarms.

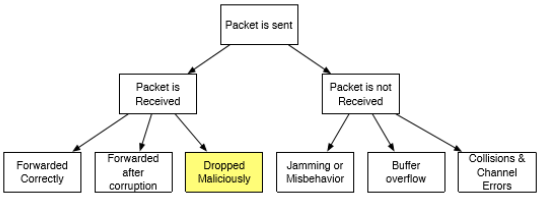

Figure 2: Overview of packet drop attack

Under the system and adversary models used earlier, the problem address was of identifying the nodes on an arbitrary path that drop packets maliciously. There is requirement for the detection to be performed by a public auditor that does not have knowledge of the secrets held by the nodes on that path. When a malicious node is identified, the auditor should be able to construct an openly verifiable proof of the misbehavior of that node.

Secondly, a malicious node that is occurred on the route can exploit its information of the network protocol and the communication context to launch an insider attack–an attack that is intermittent, but can achieve the network performance degradation. Detecting selective packet-dropping attacks is extremely challenging in a highly dynamic wireless environment. The difficulty comes from the requirement that we need to not only detect the place (or hop) where the packet is dropped, but also describe whether the drop is intentional or unintentional. E.g. fading, noise and interference which are also known as link errors.

- In multi-hop wireless Ad-hoc network; there are two types of packet losses that are link error and malicious packet dropping.
- With earlier techniques, there was poor Signal to Noise Ratio which exhibits the ratio of useful information to false or irrelevant data.
- In case of transmission of immense size data, there is requirement of more storage which makes the system more complex.

V. METHODOLOGY

Step 1: The GUI (graphic user interface) creation of the wireless nodes; intermediate nodes, source node and destination node in the editor window of the MATLAB.

Step 2: Now the bitmap of each node is obtained when the transmission is starts of packets from source node to destination node. The range of the bits is determined by bitmap and it can be zero or ones.

Step 3: In this step a fixed value of hash function is produced by HLA algorithm which is used for data authentication and integrity.

Step 4: In this step, data which is send by the source to destination is encrypted with Triple DES algorithm so as to secure data transmission.

Step 5: In this step, data is decrypted with Triple DES and RSA algorithm and calculate the probabilities of messages which are received at their destinations with or without error are also calculated. The comparison between existing technologies with introduced technologies also calculated.

VI. CONCLUSION

Wireless sensor network is a self-configuring ad-hoc network in which small nodes communicating among them using radio signals and monitor physical and environmental condition. Many routing protocols have been designed for ad-hoc networks. However, sensor networks have additional requirements that were not specifically addressed. These include real-time requirements and nodes which are extremely constrained in computing power, bandwidth, and memory. In wireless sensor network nodes are present in hostile or dangerous environment in that environment, they are not physically protected. A various types of attacks are possible in Wireless Sensor Network (WSN). Wireless sensor node network means that shares common property as a computer network. So we need security issues, for security we need secure resource or information we need integrity, availability, or confidentiality of a system.

REFERENCES

[1] Igor Ganichev, Bin Dai and P. Brighten Godfrey, "YAMR: Yet Another Multipath Routing Protocol" ACM SIGCOMM Computer Communication Review Volume 40, Number 5, October 2010.

[2] Mohammad Masdari and Maryam Tanabi, "Multipath Routing protocols in Wireless Sensor Networks: A Survey and Analysis" International Journal of Future Generation Communication and Networking Vol.6, No.6, 2013.

[3] Yi Ren, Vladimir Oleshchuk, Frank Y. Li and Xiaohu Ge, "Security in Mobile Wireless Sensor Networks - A Survey" Journal Of Communications, Vol. 6, No. 2, April 2011.

[4] Fujian Qin, and Youyuan Liu, "Multipath Routing for Mobile Ad Hoc Network" International Symposium on Information Processing (ISIP'09), Huangshan, P. R. China, August 21-23, 2009, pp. 237-240.

[5] M. Srbinovska, V. Dimcev, C. Gavrovski and Z. Kokolanski, "Localization Techniques in Wireless Sensor Networks using Measurement of Received Signal Strength Indicator" Electronics, Vol. 15, No. 1, June 2011.

[6] F. Akyildiz and I.H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges," Ad Hoc Networks, vol. 2, no. 4, pp. 351-367, Oct. 2004.

[7] F. Hu and X. Cao, "Wireless Sensor Networks: Principles and Practice", Auerbach, Boca Raton, Fla, USA, 1st edition, 2010.

[8] S. Qureshi, A. Asar, A. Rehman, and A. Baseer, "Swarm intelligence based detection of malicious beacon node for secure localization in wireless sensor networks," Journal of Emerging Trends in Engineering and Applied Sciences, vol. 2, no. 4, pp. 664–672, 2011.

[9] Masadeh, S.R. Aljawarneh,S.; Turab, N.; Abuerrub, A.M, "A comparison of data encryption algorithms with the proposed algorithm: Wireless security", Networked Computing and Advanced Information Management (NCM), 2010 Sixth International Conference.

[10] M. Caytiles, R. Gelogo, Y.;Tai-hoon Kim, "Comparison of Encryption Schemes as Used in Communication between SCADA Components Ubiquitous Computing and Multimedia Applications (UCMA)", International Conference on Robles, R.-J. Dept. of Multimedia Eng., Hannam Univ., Daejeon, South Korea Balitanas, 2011.

[11] Acharya, B. Jena, D. Patra, S.K. Panda, G, "Invertible, Involutory and Permutation Matrix Generation Methods for Hill Cipher System Advanced Computer Control", ICACC '09. International Conference on IEEE Conference Publications, 2009.

[12] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud "Evaluating the Effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types" International Journal of Network Security, Vol.11, No.2, PP.78-87, Sept, 2012

[13] Simar Preet Singh, and Raman Maini "Comparison of Data Encryption Algorithms" International Journal Of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127

[14] Challa Narasimham, Jayaram Pradhan, "Evaluation Of Performance Characteristics Of Cryptosystem Using Text Files", Journal of Theoretical and Applied Information Technology,pp55-59 2008.

[15] Abdel-Karim Al Tamimi, "Performance Analysis of Data Encryption Algorithms", International Journal Of Computer Science and Communication Vol. 2, No. 1, 2013