ISSN: 0975-833X

Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 09, pp.73259-73262, September, 2018

DOI: https://doi.org/10.24941/ijcr.32352.09.2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

RESEARCH ARTICLE

NOVEL APPROACH FOR MALICIOUS NODE DETECTION IN WIRELESS SENSOR NETWORKS

*Rajput

Department of Computer Science Engineering (M.Tech)

ARTICLE INFO

Article History:
Received 24th June, 2018
Received in revised form
27th July, 2018
Accepted 20th August, 2018
Published online 30th September, 2018

Key Words:
Sinkhole,
Malicious, WSN

ABSTRACT

A network that deploys numerous sensor nodes that use wireless mode for communication amongst each other is known as a wireless sensor network. The nodes are self-configuring in nature due to which the security of these networks is a major issue. The types of malicious nodes present in the network result in causing either passive or active types of attacks in these networks. This research proposes a study related to an active type of attack known as sinkhole attack. There is reduction in the overall lifetime of the network and increment in the amount of energy being consumed when sinkhole attack occurs. A new approach is proposed here for detecting the malicious nodes that are responsible of causing sinkhole attack in WSNs.

Citation: *Rajput*, 2018. "Novel Approach for Malicious Node Detection in Wireless Sensor Networks", *International Journal of Current Research*, 10, (09), 73259-73262.

INTRODUCTION

A network that is deployed with large number of sensing devices that are of small size and are less costly is known as a wireless sensor network (WSN). From the surrounding regions, the information is collected by these sensing devices which are also known as sensor nodes. At first, the military applications were the first that identified the need to introduce such networks since these areas were large and it was humanly impossible to monitor such areas at all times (Anitha, 2013). Today, these networks have been deployed in all the areas ranging from civilian applications to the healthcare applications. In order to collect the real time data from the surrounding regions, the small sized sensor nodes are densely deployed over the areas by WSN. The wireless sensor networks have several such unique characteristics which make them very different from other. However, they are likely to face various attacks as well. Due to the broadcasting provided in WSNs, these networks are highly vulnerable and susceptible to different types of security attacks. Further, the areas in which these networks are deployed are highly hostile and dangerous due to which the attacks are easy to enter in them. The functions performed by the sensor nodes are very different and these nodes are distributed within the overall system such that the information can be collected from every area. The regions are monitored in a very cooperative fashion and in order to perform overall analysis, the data is calculated further (David, 2008).

Aggregation and base station are the two important components of WSNs. The information is gathered from the surrounding sensors and integrated by the aggregation. In order to process this information, this data is passed on to the base station (Chris Karlof, 2003). Since these networks are deployed in hostile areas and there are limited numbers of resources available, there is unprotected and unsafe type of communication provided by WSNs. Within WSN, it is not sufficient to provide many of the security techniques. Also, security plays a very important role within these networks. Due to the unique properties of WSNs, there are several challenges being faced in terms of their security. There is a fundamental need to provide security within wireless sensor networks which also has particular requirements to be available. The bounded resources of each sensor node are achieved along with the guarantee that the sensitive data will be protected with the help of these requirements. The sensor networks are thus kept alive with the help of these functionalities. An attacker can possibly attack the networks due to the vulnerabilities and opportunities present in them. The wireless sensor networks have several such unique characteristics which make them very different from other (Yan Sun, 2008). However, they are likely to face various attacks as well. Due to the broadcasting provided in WSNs, these networks are highly vulnerable and susceptible to different types of security attacks. Further, the areas in which these networks are deployed are highly hostile and dangerous due to which the attacks are easy to enter in them. Within different layers of the network like physical, transport, link, network and application layers, different types of attacks are possible. There are no security techniques provided within various routing protocols and thus, the security can easily be

****Corresponding author:*** **Rajput,**
Department of Computer Science engineering (M.Tech).

breached by the attackers in these networks. The sensor network is destructed or destroyed when such intended attack is generated by the opponent. The functionality of the sensor network is limited or eliminated below the expectations due to the presence of DoS attack. Within any one of the OSI layers of WSN, this attack is possible (Yanli, 2011). The resources can be consumed such that the infrastructure configuration can be destructed in case when the efficiency of the targeted networks is interrupted by DoS. The network components are completely destroyed physically due to this attack. The wireless transmission can be disrupted due to the presence of Denial of service attack. At the receiver end, the noise, collision or interference is generated within this attack. The hello packets that are utilized for neighbor discovery are sent or replayed by the attack using high transmission power and the attack caused is known as hello flood attack. An illusion such that a node is neighbor of the other nodes is generated by the attacker here (Xu, 2005). This would cause the disruption of routing protocol involved and result in causing more attacks in that network. For encouraging the sensors within the networks, the Hello packet is used as a weapon by the attacker. A Hello packet is transmitted to several sensor nodes by the attacker that has higher radio transmission range as well as the processing power. Further, within huge areas, these nodes are divided. In order to make sure that the packets can be transmitted from one end to the other at higher speed using multi-hops, a low-latency link is generated within the network which results in generating the wormhole attack.

Complete and accurate sensing data is prevented to be achieved from the base station when sinkhole attack is caused. Thus, towards the higher-layer applications, a serious threat is generated by this attack. The complete traffic from the area can be attracted by the attacker from the sinkhole attack. By making the malicious node look highly attractive for other surrounding nodes along with the routing protocols involved, sinkhole attack is generated (Xu, 2007). It is not possible for the base station to achieve completely correct sensing data with the presence of sinkhole attack in the network. Thus, the higher layer applications face huge threat due to the presence of such attacks. All the traffic from a specific region is to be attracted towards the adversary node in a sinkhole. Due to the presence of adversary at the center, a metaphorical sinkhole is generated here. The information from any other neighboring node is attracted by the compromised node. Therefore, each of the information that is being transmitted to the neighboring sensor nodes is eavesdropped by the sensor node. By making a compromised node look as highly attractive to the neighboring nodes as per the routing algorithm, the sinkhole attack is generated. For instance, for providing a high quality of route towards the base station, it is possible to spoof the adversary.

Literature Review: Wei Li, et.al (2017) presented the wireless sensor network in this the security issue is faced in the physical layer in the presence of passive eavesdroppers. They proposed the two optimal power allocation strategies in this paper utilized for both power constrained and power unconstrained systems respectively (Wei, 2017). The main objective is the minimization of the secrecy rate outage probability for the power constrained system. But, in order to minimize the total power under the quality of service and secrecy constraints, they obtain the optimal power allocation for power constrained system. In the different positions of eavesdropper, they considered the secrecy outage probability. They performed simulation in order to check the performance of the proposed strategies in comparison to others. Praveena, et.al (2017) presented a new symmetric encryption standard algorithm in this paper, which is the extended form of the previously used method such as UES version-II and III (Praveena, 2017). They developed some efficient encryption methods such as UES version-I, Modified UES-I, UES version-II, UES version-III. This new version proposed named as Ultra Encryption Standard version – IV algorithm. There are multiple encryption are included in the Symmetric key Cryptosystem such as bit-wise reshuffling method and bit-wise columnar transposition method. At the bit-level, they performed the encryption process within the proposed work in order to attain greater strength of encryption. Therefore, it is concluded that this method has been utilized for the encryption of short messages, password or any confidential key. Janhavi Kulkarni, et al. (2017) presented for the security implementation in low cost wireless sensor networks, they utilized the On-chip cryptographic units in this paper. They proposed a method in this paper which ensures that present information is secured and safe in which simple radio transreceiver is used for communication by minimizing the processing time extensively. In order to test they utilized a test platform such as off-the- shelf SoC (NXP MK64Fx series) with an on-chip memory mapped cryptographic unit (Janhavi Kulkarni, 2017). It is also seen by increasing the processing time in the system, it becomes possible to secure the core protocol stacks of simple radio transreceivers. Therefore, with the help of this approach, greater flexibility in controlling the security parameters is attained and also provides the greater optimization of the system.

Aditi Rani et al. (2017) presented sensor nodes are deployed in the wireless sensor networks and are distributed randomly within the network using which data is gathered from the physical or environmental conditions like sound, stress waves, temperature of surrounding (Aditi Rani, 2017). There are various applications in which the technology of WSNs has been utilized such as military areas, disaster management in remote areas, hospital, building smart cities and many more. Hence, an important role is played by the security in the WSNs applications. These networks are easily maligned to the various disastrous attacks or hackers in order to breakdown the whole network. They observed the various aspects of security in wireless sensor networks like cryptography, security at the node level in the network and routing protocols security and many more. Najmus Saqib et al (2016) presented the widespread application of the wireless sensor network due to which it is utilized in almost all the applications. It is an active area for the research due to its vast applications. Due to the issue of resource constraint in the traditional security protocols, they are not utilized in the present networks. The low computational overhead is present in the ECC due to which it is considered as a viable cryptographic technique. They carried out the detailed study on the ECC of a popular WSN operating system. They utilized the TinyECC library, for the practical implementation of the ECC operations (Najmus Saqib, 2016). In order to develop the custom security protocols on TinyOS, they utilized the TinyECC in this paper. They also evaluated the performance of the proposed method. MicaZ Motes were used in order to fuse the developed protocols. Walid Elgenaidi et al (2016) presented the cryptographic mechanisms in this paper using which security in Wireless Sensor Networks can be handled optimally (Walid Elgenaidi, 2016). But in case of sensor nodes low memory and low computation capability are the major issues. There are some major issues such as memory and storage space, key generation, and re-keying in the WSNs which are minimized by the tools of trust management schemes. In order to obtain a secure maritime coastal monitoring system, they presented various solutions to the issues of memory resources consumption and key management processing. On the basis of the trusted node configuration, this system is based called as a symmetric security scheme with a dynamic update key. It is also known as the leader node which relies upon the third party.

RESEARCH METHODOLOGY

The malicious nodes are responsible for the reduced performance of the networks. This malicious node creates different types of active and passive attack on the sensor nodes by just entering inside the networks. Sinkhole is one the major active attack in which the attacker floods all the data and information out from the network due to which the sensor nodes are busy in replying the route packets. Mutual authentication of sensor nodes and isolation of malicious nodes are proposed in this research paper. The methodology works according to below mentioned steps:-

Step 1: The network is consisting of enormous number of sensor nodes.
Step 2: During the execution of loop for every node in the network.

Step 2.1 The location of node is detected by base station with the help of node localization process.

Step 2.2 Each node has assigned a unique arm strong number by the base station.

Step 2.3 Also a unique ID code is assigned to every node in the network by the base station. While End

Step 3: The process of cluster heads is initiated in the network.

The nodes which are selected as the volunteer node are selected as the cluster head.

The unique ID and arm strong number is send to the volunteer node by the base station.

When all the loops are executed,

Step 3.3.1 Then all the information is matched.

RESULTS

The proposed research work has been implemented in MATLAB and the results are evaluated by making comparison amongst proposed and existing approach in terms of several parameters. Comparisons are made in terms of packet loss ratio achieved amongst the proposed, traditional LEACH and the LEACH applied in network with sinkhole attack. The results shown graphically clearly depict that there is minimum packet loss achieved in the improved proposed network. Comparisons are made amongst proposed, traditional LEACH and the LEACH applied in attack scenario in figure 3. It is seen that with the elimination of sinkhole attack from WSNs, there is reduction in amount of energy being consumed. Comparative analysis against proposed and traditional approaches is done in terms of throughput achieved.

The node is selected as cluster head

Else

Node gets isolated

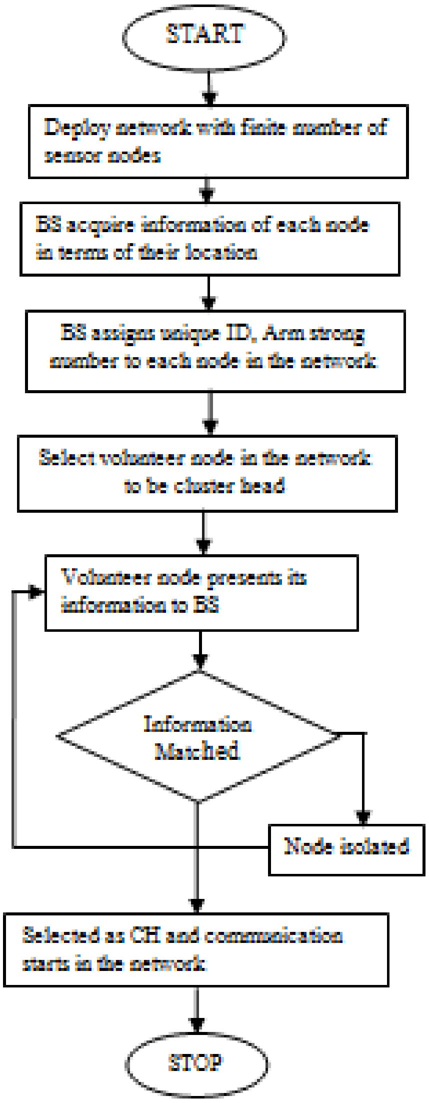
START
Deploy network with finite number of sensor nodes
BS acquire information of each node in terms of their location
BS assigns unique ID, Arm strong number to each node in the network
Select volunteer node in the network to be cluster head
Volunteer node presents its information to BS
Information Matched
Node isolated
Selected as CH and communication starts in the network
STOP

Fig. 1. Proposed Flowchart

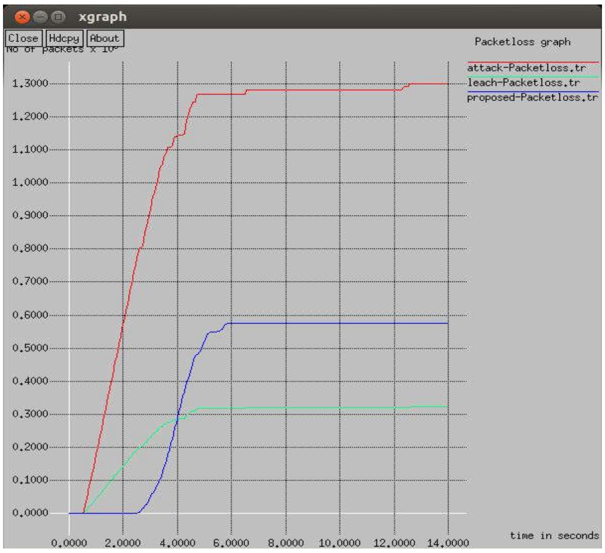

Fig. 2. Packet loss comparison

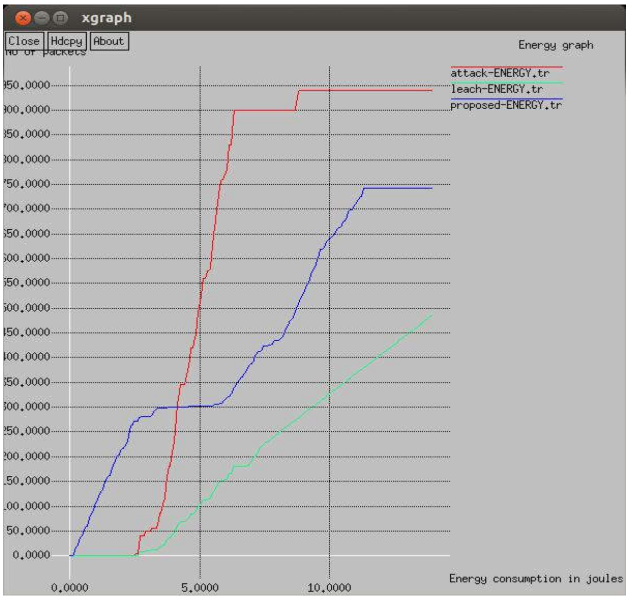

Fig. 3. Energy Comparison

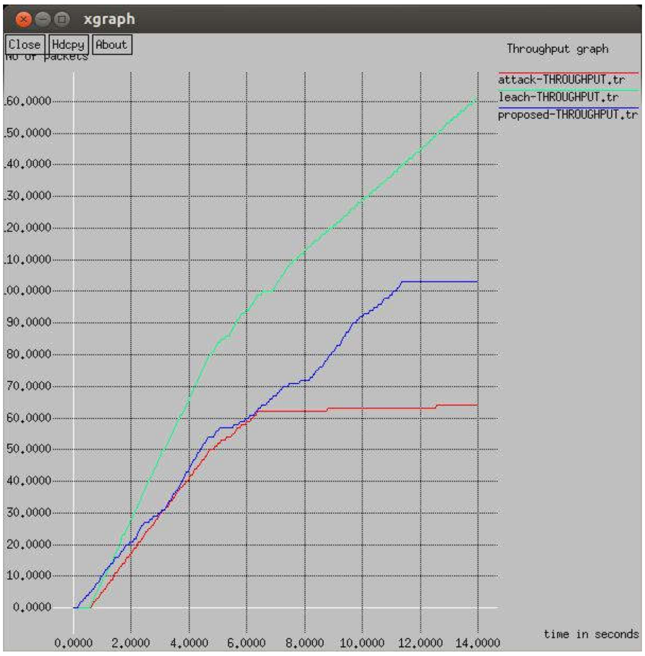

Fig. 4. Throughput Comparisons

The results are shown graphically above in figure 4. It is seen that the elimination of sinkhole attack results in increasing the throughput at steady rate.

Conclusion

Through this paper, it has been concluded that the LEACH protocol has the most effective results in terms of reduced energy consumption of WSN. The network which is used to sense the environmental conditions by making use of sensor nodes s called wireless sensor nodes. The information which is sensed by the sensor nodes are is collected and passed o the base station. As, the size of sensor nodes is very small due to which the lifetime of sensor node is also very less and the battery life is also very less. As, the sinkhole is active type of attack hence, it is responsible for the reduction in performance of the LEACH protocol. The technique of mutual authentication is introduced in this respective thesis work. The performance is studied and evaluated in terms of packet loss which is minimized by 15%, energy consumption of network is reduced to 18% and network throughput is increased by 25%.

REFERENCES

Anitha, S.Sastry, Shazia Sulthana and Dr.S Vagdevi, "Security Threats in Wireless Sensor Networks in Each Layer", *International Journal of Advanced Networking and Applications*, Vol. 04 Issue 04, pp. 1657-1661, 2013.

David R. Raymond and Scott F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", IEEE Pervasive Computing, Vol. 7, No. 1, pp. 74-81, 2008.

Chris Karlof and David Wagner, "Secure routing in wireless sensornetworks: attacks and countermeasures," Ad Hoc Networks Journal, Vol.1, Issue 2-3, pp. 293-315, 2003.

Yan Sun, Zhu Han, and K. J. Ray Liu, "Defense of Trust Management Vulnerabilities in Distributed Networks," IEEECommunications Magazine, Vol 46, Issue 2, pp.112-119, 2008.

Yanli Yu, Keqiu Li, Wanlei Zhou, and Ping Li, "Trust mechanisms in wireless sensor networks: attack analysis and countermeasures," Journal of Network and Computer Applications, Elsevier, 2011.

Xu, W. et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," MobiHoc '05: Proc. 6th ACM Int. Symp. Mobile Ad Hoc Net. and Comp., pp. 46–57, 2005.

Xu, W., W. Trappe, and Y. Zhang, "Channel Surfing: Defending Wireless Sensor Networks from Interference", in Proc. Of Information Processing in Sensor Networks, 2007.

Wei Li, Kexiong Liu , Sixin Wang , Jing Lei , Erbao Li , Xiaoqian Li, "Full-duplex Relay for Enhancing Physical Layer Security in Wireless Sensor Networks: Optimal Power Allocation for Minimizing Secrecy Outage Probability", 2017 17th IEEE International Conference on Communication Technology

Praveena, A. "Achieving Data Security in Wireless Sensor Networks Using Ultra Encryption Standard Version – IV Algorithm", IEEE International Conference on Innovations in Green Energy and Healthcare Technologies 2017

Janhavi Kulkarni, Karan Nair, Aditya Pappu, Sarthak Gadre, Ganesh Gore, Jonathan Joshi, "Using On-Chip Cryptographic Units for Security in Wireless Sensor Networks", IEEE, 2017

Aditi Rani, Sanjeet Kumar, "A Survey of security in Wireless Sensor Networks", 3 rd IEEE International Conference on "Computational Intelligence and Communication Technology"2017

Najmus Saqib, Ummer Iqbal, "Security in Wireless Sensor Networks using ECC", 2016 IEEE International Conference on Advances in Computer Applications,

Walid Elgenaidi, Thomas Newe, Eoin O'Connell, Daniel Toal, Gerard Dooly and Joseph Coleman, "Memory Storage Administration of Security Encryption Keys for Line Topology in Maritime Wireless Sensor Networks", 2016 Tenth International Conference on Sensing Technology

****