International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 54-58
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

COMPARATIVE STUDY AND ANALYSIS OF BYZANTINE ATTACK WITH PREVENTION TECHNIQUE

Shivali Goyal, Gurdeep Kaur
Department of IT
CEC Landran, Mohali

Dr. Parminder Singh
Department of IT
CEC, Landran, Mohali

ABSTRACT: Information or messages carrying by the high end devices and flow in large scale networks. This is not a message flaw, but simply reflects the large number of data which could be scrutinized by the high end machines. The main problem of network is lack of security between the information; thus, information will have seen by any host machine. Nearly millions of data used in the Internet today, but high end technologies never provide any surety on the network. Currently, we are working on the network attacks and byzantine attack is out of them that disrupt the information. The sensor node is testified before a network allow to enter in the authorized area. If the node had communicated in the network then it is allowed by the base station node.The base station continue to search inside the network and if identified the attacker-- the base station node was stepped to terminate the node up on the network.

Keywords: **byzantine attack, Wireless sensor network (WSN)**

I. INTRODUCTION

The traffic in Wireless Sensor Network depends on number of queries generated per Mean time. The sink node transmits the information to be sensed by sending a query throughout the sensor field. The sensor nodes respond to the query by gathering the data using their sensors. Ultimately when the sensor nodes have the result of the injected query will reply to the sink node through some routing protocol. A sensor node also aggregates the replies to a single response which saves the number of packets to send back to the sink node[4]

A. Security issues

In networks there is many hazard and attacks against the security which are almost similar to their wired counterparts. In fact, wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In most of the cases various security issues and threats related to those we consider for wireless ad hoc networks are also applicable for wireless sensor network [20].
We are now improving these security issues so that sensor nodes provide the security on the network i.e.

1. **Confidentiality**: In Wireless sensor network the data is communicated from one node to another node and after routing through many nodes, the data or information is passed to the base station. It is important that any message routed through wireless sensor network is confidential and not accessible to unauthorized user.
2. **Authentication:** It may possible that unauthorized access by some malicious node may drop some packets from network or may introduce some false packets into the network. Such unwanted affects can be avoided if we have some means to identify the original sensor nodes.
3. **Integrity:** The alteration done in data packets by malicious node violates the concept of integrity. Integrity means to ensure the correctness of the data. Receiver node should receive the data in original as send by the sender node.
4. **Availability:** Failure of a node may leads to failure of a path or failure of base station may leads to failure of entire networks. Sensor nodes and base station should always be available to provide services of Wireless sensor networks.
5. **Freshness:** The data of each message should have freshness i.e. data should be recent; no old data should be replayed by malicious nodes.
6. **Time Synchronization:** Most of the Wireless sensor network uses time synchronization to calculate the delay between packets in a pair of two nodes.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 54-58
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

B. Attacks in Wireless Sensor Network

Security issue is the main concern in sensor network. These attacks are as follow:

1. **Worm hole Attack:** This attack is based on network layer. In this attack malicious node recording all the packets at every location in the network and then make tunneling to pass all the packets from one node to another node. The solution to this problem is monitoring the network and flexible routing schemes.
2. **Black hole Attack:** InBlack-hole attacks malicious node captures and re-programs a set of nodes in the network and blocks the packets they receive instead of forwarding them towards the base station. Any packet that enters into the black hole region is captured by the malicious node and never reaches the destination node. [7, 8]
3. **Denial of Service Attack:** This malicious node in this attack hits on the accessibility of a node and all nodes in the whole of the network. Aim of this attack is to block the services of the sensor nodes [7, 8]. The attacker generally uses battery exhaustion method and radio signal jamming. It has further different categories:
    a Reflected Attack
    b Peer to peer attacks
    c UDP flood attack
4. **Byzantine** Attack: In this attack nodes are compromised to each other due to this packets are drop continuously and behave like normal node. When packets are continuously dropping then it creates a collision in the network and also degrades the performance of the network. It makes a different routing path in the network.

II. LITERATURE SURVEY

Ju young Kim and Ronnie D. Caytiles (2013)presented a study of the different vulnerabilities, threats and attacks for wireless sensors networks[7]. Effective management of the threats associated with wireless technology requires a sound and through assessment of risk given the environment and development of a plan to mitigate identified threats. An analysis to help network managers understand and asses the various threats associated with the use of wireless technology and a number of available solutions for countering those threats are discussed. Wireless sensors networks provide a numerous opportunities for increasing productivity and minimizing costs. It provides significant advantages for many applications that would not have been possible for the past. The different vulnerabilities threats and attack that could possibly put WSNs in a vital or critical situation have been identified and discussed in this paper. The different categories of these threats are defined to identify a possible countermeasure scheme applicable for each threat classification.

TeodorGrigore LUPU (2012) presented that security has become the forefront of network management and implementation [9]. The challenge in security issues to find a well balanced situation between two of the most important requirements: the need of developing networks in order to sustain the evolving business opportunities and work level, and the need to protect classified, private and in some cases even strategic information. The application of an effective security policy is the most important step that an institution can take to protect its network. Networks have grown in both size and importance in a very short period of time. If the security is compromised, there could be serious consequences of wireless sensor network.

Aditya Vempaty (2013) introduced that the control of the false discovery rate (FDR) for distributed detection in wireless sensors network (WSNs) can provide substantial improvement in detection performance over convential design methodologies [11]. In this paper, further investigate system design issues in FDR-based distributed detection. They demonstrate that improved system design may be achieved by employing the Kolmogorov- Smirnov distance metric instead of the deflection coefficient. They also analyze the performance of FDR based distributed detection in the presence of byzantine.Byzantines are the malicious sensors which send the falsified information to the fusion center (FC) to deteriorate system performance. It is observed that detection performance is degrading when fraction of Byzantines is large. Detection simulation results are providing to demonstrate the robustness of the proposed adaptive algorithm to byzantine attacks in WSNs.

Chris Karlof, David Wagner (2003) considered [12] routing security in wireless sensors networks. Many sensors network routing protocols have been proposed but none of them have been designed with security as a goal. They proposed security goals for routing in sensor networks, show how attack against ad-hoc and peer-to peer networks can be adapted into powerful attacks against the sensors networks, introduce two classes of novel attacks against the sensors network like sinkholes and HELLO floods and, analyze the security of the entire major sensors network routing protocols.

III. AFFECTS OF BYZANTINE ATTACK

When the malicious node is triggered in the network then the performance of the network is degrade then performance metrics is improved by packet delivery ratio, end to end delay and packet loss ratio.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 54-58
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

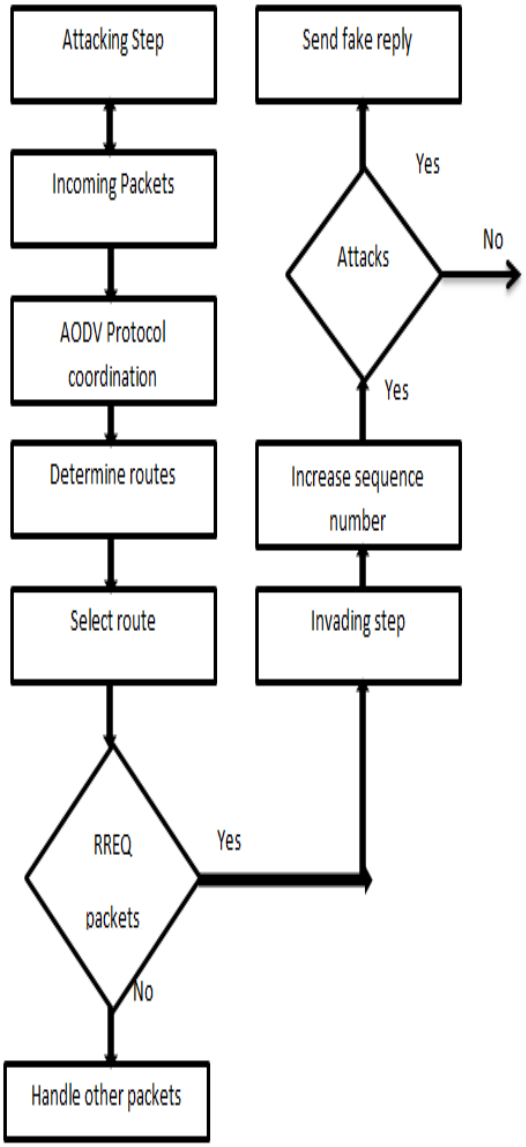

FIGURE 1.1 ATTACK GENERATION [2]

IV. PROPOSED SUGGESTIONS

The proposed technique is based on trust values. In this techniques adjacent nodes of each node is calculated and nodes which can change its identification its trust value reduced according to time. The nodes which have least trust value is detected as malicious nodes in the network.
The first step of the technique is to gather in information about the location and adjacent nodes of each node.
The second step is the assign trust values to each node. The node which change identification has different adjacent nodes each time, this information will reduce the trust value of the node.
The node which have minimum trust value will be detected as the malicious nodes and it will isolated from the network

V. SIMULATION AND RESULTS

A. Packet drop

This parameter is mostly used in security attacks and research community of networking. This term refers that packets are releasing in the network. Due to reason of making non optimal paths are made in the network and stealing the information in form of packets. Due to packet loss routers lost the path and it also degrades the network performance.

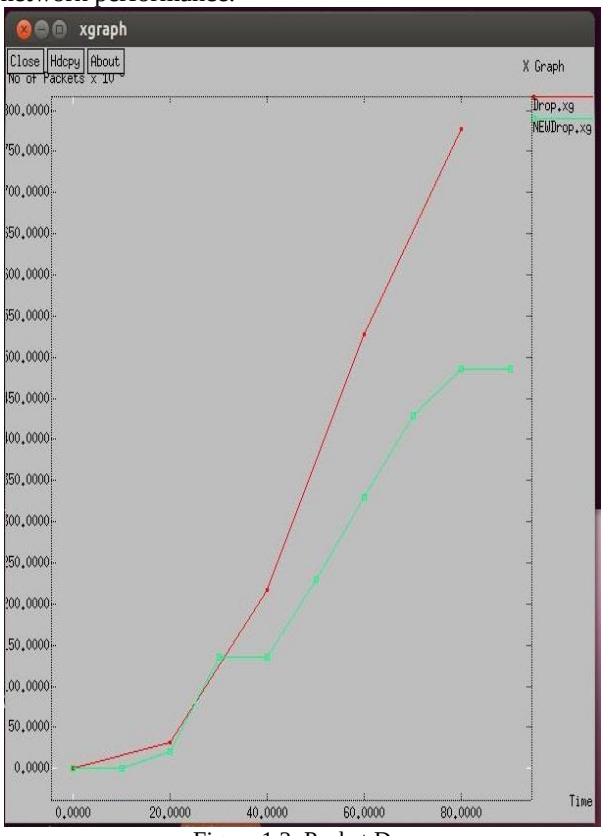

Figure 1.2: Packet Drop

B. Throughput

This term means that how much messages are successfully reached in the network. It does not matter whether the messages are delivered through physical or logical link. If the messages are successfully reached according to simulation time then throughput of the network is high.

International Journal of Engineering Applied Sciences and Technology, 2016
Vol. 1, Issue 9, ISSN No. 2455-2143, Pages 54-58
Published Online July – August 2016 in IJEAST (http://www.ijeast.com)

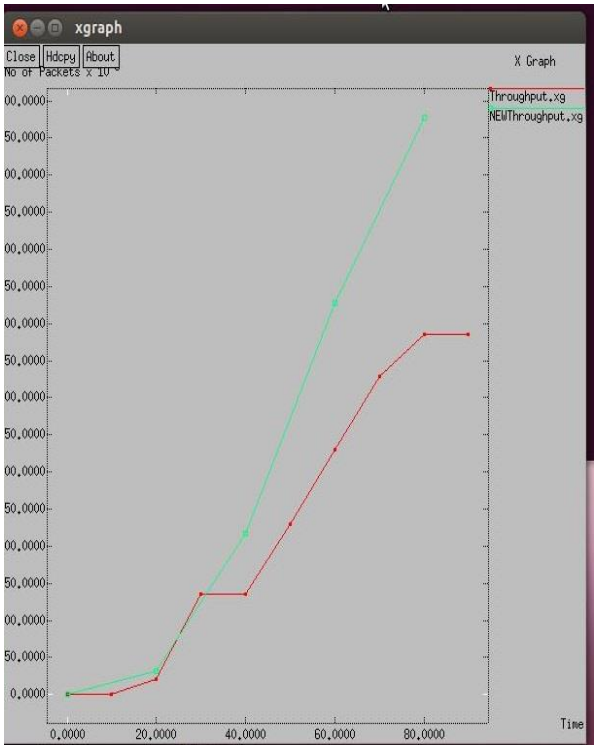

Figure 1.3: Throughput

VI. CONCLUSION

Centralized Base Station node alert about the attacker node; by now more or less certain their paths was same network. Due to decentralized nature of WSN bidirectional attack is possible in the network which is triggered by the malicious node. The simulation results show that Throughput, packet loss increase due to byzantine attack. The proposed scheme is based upon trust values and improving the drop ratio and thus throughput is high.

VII. REFERENCES

[1] Jen-Yeu Chen and Yi-Ying Tseng, "Distributed Intrusion Detection of Byzantine Attacks in Wireless Networks with Random Linear Network Coding", IEEE, 2013

[2] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009, pp. 1-9

[3] G.H. Raghunandan, B.N. Lakshmi, "A Comparative Analysis of Routing Techniques for Wireless Sensor Networks", Proceedings of the National Conference on Innovations in Emerging Technology,IEEE 2011.

[4] UdayaSuriya Raj Kumar Dhamodharan and RajamaniVayanaperumal [3], explained in their paper , "Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method, Hindawi Publishing Corporation theScientific World Journal Volume 2015, Article ID 841267, 7 pages

[5] Ahmad Salehi S., M.A. Razzaque, ParisaNaraei, Ali Farrokhtala, " Detection of sink hole Attack in wireless sensor networks",IEEE International Conference on Space Science and Communication (IconSpace), 1-3 July 2013, Melaka, Malaysia, pp. 361-365

[6]I.F.Akyildiz,W.Su,Y.Sankarasubramaniam, E.Cayirci. "WirelessSensorNetworks:Asurvey" Broadband and Wireless Networking Laboratory, School of Electrical and Computer Engineering,Georgiainstituteof Technology,Atlanta,GA30332,USAReceived12Decembe r2001; accepted20 December2001, pp . 392-422.

[7] Stefano Marano, Vincenzo Matta, and Lang Tong, "Distributed Detection in the Presence of Byzantine Attacks", IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 57, NO. 1, JANUARY 2009

[8] Kalpana Sharma and M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats"IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010, pp.42-45

[9] Baruch Awerbuch , Reza Curtmola, David Holmer , Cristina Nita-Rotaru and Herbert Rubens, "Mitigating Byzantine Attacks in Ad Hoc Wireless Networks", 2009

[10] NisargGandhewar, Rahila Patel, "Detection & Prevention of Sybil Attack on AODV Protocol in Mobile Adhoc Network", Fourth International Conference on Computational Intelligence and Communication Networks, IEEE, 2012, pp. 714-718

[11] Hero Modraes, RosliSalleh and AmirhosseinMoravjosharieh, "Overview of Security Issues in Wireless Sensor Netowrks", Third International Conference on Computational Intelligence, Modeling and Simulation (CIMSiM), IEEE 2011, pp. 308-311

[12] Vinay Soni, Pratik Modi, VishvashChaudhri, "Detecting Sinkhole Attack in Wireless Sensor Network", International Journal of Application Volume 2, Issue 2, February 2013

[13] Chun-Hsin Wang and Yang-Tang Li, "Active Black Holes Detection in Ad-Hoc Wireless Networks", IEEE, 2013

[14]Teodar-Grigopou, "Main Types of Attacks in Wireless Sensor Network", Recent Advances in Signals and Systems, ISSN: 1790-5109, 2009

[15] ADITYA VEMPATY, PRIYADIP RAY, PRAMOD K. VARSHNEY (2014) proposed in their paper, "False Discovery Rate Based Distributed Detection in the Presence of Byzantines", IEEE TRANSACTIONS ON AEROSPACE AND ELECTRONIC SYSTEMS VOL. 50, NO. 3 JULY 2014

[16] Dr. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and

Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 200

[17] Kalpana Sharma and M K Ghose, "Wireless Sensor Networks: An Overview on itsSecurity Threats" IJCA Special Issue on "Mobile Ad-hoc Networks"MANETs, 2010

[18] LV Shaohe,WangXiaodong, ZhaoXing, Zhou Xingming , " Detecting the Sybil Attack Cooperatively in Wireless Sensor Networks", Computational Intelligence and Security 2008,CIS '08 International Conference on Volume 1Suzhou, pp.442-446, IEEE 2000

[19] Baviskar B.R, Patel V.N," Black hole attacks mitigation and prevention in wireless sensor network", International Journal of Innovative Research in Advanced Engineering (IJIRAE), Volume 1, Issue 4, pp.167-169,May 2014.

[20] Wang Chun-Hsin and Li Yang-Tang, "Active Black Holes Detection in Ad-Hoc Wireless Networks", Ubiquitous and Future Networks (ICUFN) 2013 Fifth International Conference on Da Nang,pp.94-99, IEEE, 2013