IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 12, December 2015

Energy Efficient DYMO Protocol for 802.15.4 over Flooding Attack

Garima Pahare[1], Surbhi Koushik[2]

PG Scholar, Department of ECE, RGPV University, Indore, India [1]

Assistant Professor, Department of ECE, RGPV University, Indore, India [2]

Abstract: Mobile Ad-hoc Network (MANET) is a kind of wireless network having more than hundreds nodes interconnected in open nature field. A strong purpose may lead it as one of emerging and popular research field for researchers. Wireless sensor a network is widely used for real time submission at military combat zone, nuclear power plants etc. A mobile node consist small data storage capacity, low power battery, low bandwidth and low computational power. Due to open nature communication medium, it becomes more vulnerable to outside attacks. Security threats are classified in two category passive and active attacks. In passive attack attacker can listen the packets in the network while in the active attack attacker can also modify the packet contents. Subsequently, little attack may lie into both categories. Flooding attack is such kind of attack which aims to disrupt the network by draining resource capability. Here, Attacker communicates worthless messages formally known as false packet to increase network traffic and make target node busy in useless activity. The complete work observes that, Flooding attack does not require any study about network vulnerability. Furthermore, the major thread in way of development is challenges in sensor networks. Poor resources availability is the major weakness of sensor network. Attacker may use this weakness to disrupt the network. Subsequently, Power draining is the major thread; where attacker not only exhausts the network traffic but also degrades the life of node as well network. The objective of this study is to detect and prevent wireless sensor networks from unwanted power draining due to Flooding attack. Here, Targeted Flooding through high battery capacity node has been used to deploy Flooding attack in ad-hoc network. Subsequently, energy consumption and capacity observation technique has been used to detect malicious node(s). Furthermore, prevention method forcefully shutdown malicious nodes and transfer communication from another route to avoid power draining. Energy consumption before attack, during attack and after prevention along with throughput and packet delivery ratio is used to measure performance of proposed technique. NS-2 simulator has been used to simulate and evaluate the results of proposed solution.

Keywords: MANET, Flooding, DYMO, WSN.

I. INTRODUCTION

A Mobile Ad-hoc Network is a collection of independent mobile nodes that can communicate to each other via radio waves. The mobile nodes that are in radio range of each other can directly communicate, whereas others need the aid of intermediate nodes to route their packets. Each of the nodes has a wireless interface to communicate with each other. These networks are fully distributed, and can work at any place without the help of any fixed infrastructure as access points or base stations. Figure 1 shows a simple ad-hoc network with 3 nodes. Node 1 and node 3 are not within range of each other; however the node 2 can be used to forward packets between node 1and nodes 2. The node 2 will act as a router and these three nodes together form an ad-hoc network.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. This results in a highly dynamic, autonomous topology.

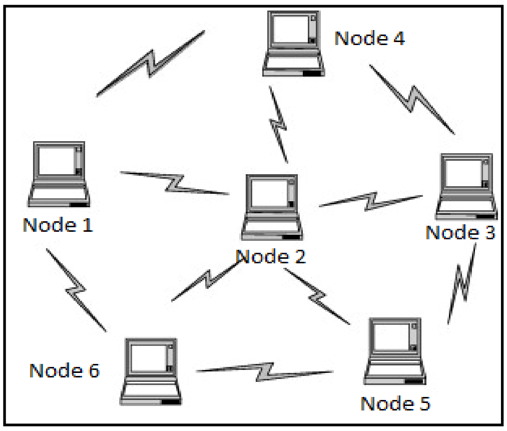

Figure 1.Example of a simple ad-hoc network with three participating nodes.

There are two distinct wireless networks for enabling wireless nodes to communicate with each other:

1. Fixed Infrastructure network
2. Infrastructure less network

The major weakness in MANET is a hardware limitation, which makes it vulnerable to many kinds of attacks. Attacker with heavy power supply, processing capabilities and good quality transmission may easily compromise the

DOI 10.17148/IJARCCE.2015.41267

sensor node to deploy wormhole attack. There are two ways of the adversary those are passive attack and active attack.

Flooding attack is defined as attacks that are launched by a set of malicious entities towards a victim, with the aim of incapacitating it from providing further service to legitimate clients. The objectives of the attack are achieved by exploiting either system/protocol-level vulnerabilities, or by forcing the victim to undertake computationally intensive tasks.[2]

On the contrary, distributed denial of service attacks are defined as flooding attacks that do not rely on any particular network or system-level weaknesses. Rather they tend to exploit the asymmetry that exists between the network line rate and the victim's processing capabilities. Distributed denial of service attacks or Flooding attack are based on the principal: "Power of many is greater than power of few" Such attacks are launched subsequent to subversion and/or compromise of legitimate client machines of the network. These compromised machines then participate in the attack process.

This work describes the efficient strategy to detect and prevent power draining in MANET. In MANET, the mobile nodes are not much in power, computation, and battery life of a node so it is very difficult to detect any attack in the network. In terms of Flooding attack, it is very difficult to detect because the nodes which are the parts of the route path between the source and destination and the nodes of wireless networks are less in power and less in memory so encryption and decryption of the packets are not possible, that is a reason why this networks needs an efficient technique to detect the attacker nodes in the networks. DYMO routing protocol will be used to send the packets in network. DYMO routing protocol is on-demand routing protocol, it search a route when source is required to send a packets to destination node..

II. DYNAMIC MANET ON-DEMAND (DYMO/AODVV2)

The Dynamic MANET On-demand (DYMO) routing protocol enables dynamic, reactive, multi-hop routing between participating nodes wishing to communicate. The revised Ad Hoc On-demand Distance Vector (AODVv2) routing protocol [formerly named DYMO] enables on-demand, multi-hop unicast routing among AODVv2 routers in mobile ad hoc networks. The basic operations of the protocol are route discovery and management. During route discovery the originating node causes dissemination of a Routing Element (RE) throughout the network to find the target node. During dissemination each intermediate node creates a route to the originating node. When the target node receives the RE it responds with RE unicast toward originating node. During propagation each node creates a route to the target node. When the originating node is reached routes have been established between the originating node and the target node in both directions.

In order to react quickly to changes in the network topology nodes should maintain their routes and monitor their links. When a packet is received for a route that is no longer available the source of the packet should be notified. A Route Error (RERR) is sent to the packet source to indicate the current route is broken. Once the source receives the RERR, it will re-initiate route discovery if it still has packets to deliver.

In order to enable extension of the base specification, DYMO defines the handling of unsupported extensions. By defining default handling, future extensions are handled in a predetermined understood fashion.

DYMO uses sequence numbers to ensure loop freedom.

There are three types of control messages in DYMO which are discussed below.

1. Route Discovery
2. Route Reply (RREP)
3. Route Maintenance

III. FLOODING ATTACK

Flooding attacks are defined as attacks that are launched by a set of malicious entities towards a victim, with the aim of incapacitating it from providing further service to legitimate clients. The objectives of the attack are achieved by exploiting either system/protocol-level vulnerabilities, or by forcing the victim to undertake computationally intensive tasks, such as exponentiation large integers for applications.

As can be seen from 2, a single victim node may be targeted with overwhelming number of incoming requests from multiple ends of the network. The attacker nodes can either be legitimate but compromised nodes operating in the network, or be a laptop-class adversary, i.e. an adversary with higher capabilities, using forged identities to generate a large set of legitimate packets for overwhelming the victim node. It is assumed that no pre-hand information is available to elude towards critical (potential victims) nodes in the network. Therefore, an adversary must have observation capabilities for a certain period of time to identify on the critical nodes in the network. Intelligent set of adversaries will launch the distributed denial of service attacks from multiple ends of the network so as to avoid being detected by a detection module observing traffic from a single point of origin in the network.

Flooding attack is one of the most easy to implement attacks. Main aim of the flooding attack is to exhaust the network resources like network bandwidth or consumption of resources of other authentic users by overburdening with computational efforts exhausting their battery power. Flooding attacks can be implemented in many ways by using RREQ packets or data packets. These flooding attacks have goal to disrupt routing and create congestion. In RREQ flooding, an attacker node floods the network by sending multiple RREQ for an unknown or non-existing IP address in the network. This may even cause routing table overflow by authentic users. These multiple RREQ forwarding increases computational burden on the authentic nodes and consume their battery power. In data flooding the attacker sends unwanted useless data packets to all other nodes in the network. In this way data flooding

DOI 10.17148/IJARCCE.2015.41267

causes congestion in the network and wastage of network bandwidth.

IV. PROBLEM DOMAIN

The AODV routing protocol is a popular reactive routing protocol in wireless networks, but DYMO routing protocol designed for better performance of the network not for security of node, secure protocols are generally designed to have features such as authentication, integrity, confidentiality and non-repudiation. For security purpose DYMO have vulnerabilities and it is easily manipulate by malicious node to destroy its network routing.

The open nature of wireless medium also makes it easy for outsider attackers to interfere and interrupt the legitimate traffic. This concept classifies the attacks into two broad categories, namely Passive and Active attacks. In Passive attack, the adversary only eavesdrop upon the packets content, while packets may get dropped or altered on way in case of Active attacks. Wormhole attack is one of the Denial of Service attacks effective on the network layer, that can affect network routing, data aggregation and location based wireless security. Flooding attack does not require scanning network vulnerability; instead it uses SYS Flooding and bulk messaging to create intentional power draining in sensor networks.

The complete work determines that, there is need to develop a scheme to avoid power draining problem in MANET to sustain node life and improve the network performance over Flooding attack.

V. PROPOSED SOLUTION

The main requirement for the proposed work is to first observe the actual performance of network in terms of energy consumption on every sensor node. Subsequently, it also requires observing the energy consumption after attack and deployment of detection and prevention technique to analyze the variation into energy consumption. A NS 2.35 simulator is used to develop and observe the performance of proposed sensor network scenario and prevention technique.

A battery model ”Liner battery” has been configured with 1200 mAhr capacity at initial stage. Furthermore, “Generic” Energy model is configured to specify energy consumption at transmission, receiving, idle and sleeping stage. A monitoring of integrate battery observation on each node to keep track about battery initialization and consumption during communication is also performed.

The simulation of the work completed in three cases (scenarios). Which are?

Case 1: Development of various homogeneous nodes scenario with original DYMO routing protocol along with battery model configuration to evaluate initial battery capacity of each node. Throughput and Packet delivery ratio is also evaluated in natural situation.

Case 2: Deployment of malicious node with 1500 mAhr battery capacity along with 20000 mW extra load has been introduce through flooding method to heavily decrease the battery power of any node coming into route of transmission. A targeted Flooding technique has been developing with extra load and generates heavy traffic into target communication route. The complete phenomena frequently degrade battery capacity of targeted node.

Case 3: A battery capacity based detection technique has been developed to detect attacker node and prevention function shutdown malicious node to overcome power draining.

VI. RESULT OBSERVATIONS

The simulation of the work completed in three scenarios.

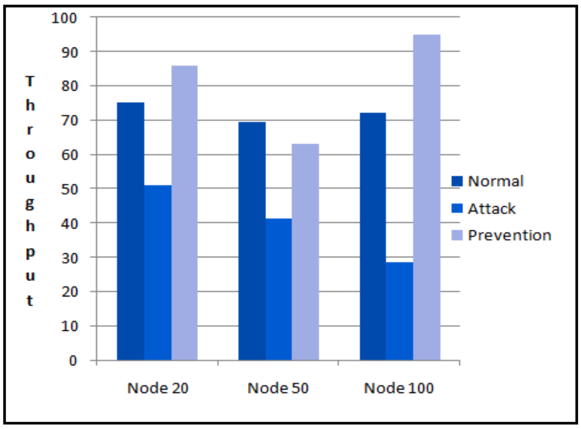

Figure 1: Comparison of Throughput

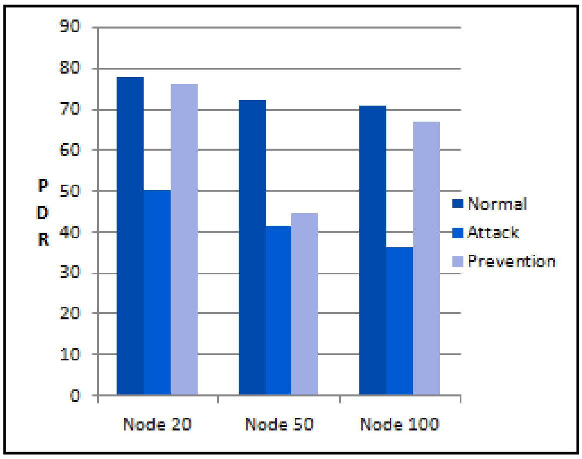

Figure 2: Comparison of PDR

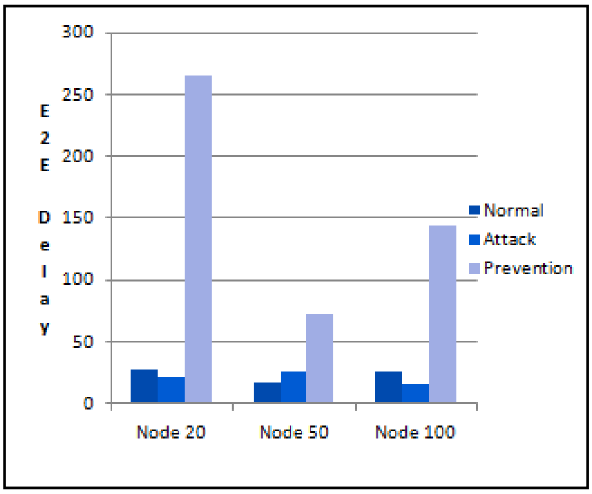

Figure 3: Comparison of E2E Delay

DOI 10.17148/IJARCCE.2015.41267

The configuration of scenarios is based on the number of nodes are deployed and the position of the source node and destination node. Initially all mobile nodes in each scenario are normal and no malicious node is present in the scenario. The standard DYMO routing algorithm is used at routing protocol on network layer. The scenarios are differentiated on the basis of number of nodes present in the scenario and the nodes are deployed in a manner that they are in the range of other nodes

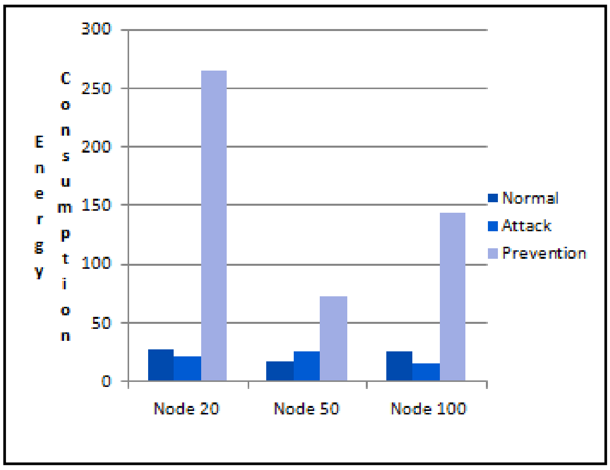

Figure 4: Comparison of Energy Consumption

VII. CONCLUSION

This study is based on detection of FLOODING attack to avoid power draining and also proposed mechanism to prevent them. The DYMO routing protocol is applied at the different network size in sensor networks. A modified DYMO routing mechanism is proposed which flooding attacker node. This algorithm also redefine route by isolating attacker node.

The results of this study show that the modified DYMO effectively detects attacker node without much degradation in energy level. The performance is measured in context of energy level. However the detection of Flooding attack and isolation of attacker node are considerable and satisfactory.

REFERENCES

[1] Sriram Nandha Premnath, Sneha Kumar Kasera, "Battery-Draining-Denial-of-Service Attack on Bluetooth Devices", Project Report School of Computing University of Utah ,2012

[2] Jaydip Sen, "A Survey on Wireless Sensor Network Security", In proceedings, *International Jouenal of Communication Networks and Information Security (IJICNIS)*, Vol 1, No 2, Augest-2009.

[3] Jayan Krishnaswami, "Denial-of-Service Attacks on Battery Powered Mobile Computers ", Master of Science in Electrical Engineering, Virginia Polytechnic Institute and State University, Blacksburg, Virginia.

[4] Maneesha V. Ramesh, "Real-time Wireless Sensor Network for Landslide Detection", In *Third International Conference on Sensor Technologies and Applications*, 09 IEEE-Computer Society of India.

[5] R.balakrishna, U.Rajeshwar Rao, N. Geetahanjali, "Performance issues on AODV And AOMDV for MANETs*", International journal of Computer Science and Information (IJCSIT),* vol. 1 (2), 2010,pp. 38-43.

[6] Miss Morli Panday,Ashish Kr. Shriwastava, "A Review on security Issues of AODV routing protocol for MANETs", *IOSR Journal of Computer Engineering(IOSR-JCE)*, e-ISSN:2278-0661, p-ISSN:2278-8727 vol. 14, Issue 5 (Sep. - Oct. 2013), pp.127-134.

[7] Sangwan,A., Sindhu,D., Singh, K., "A Review of various security protocols in Wireless Sensor Network", *IJCTA, ISSN:2229-6093*, vol. 2 (4), july-august-2011, pp.790-797.

[8] Maurice Chu, Horst Haussecker, and Feng Zhao , "Scalable Information-Driven Sensor Querying and Routing for ad hoc Heterogeneous Sensor Networks" ,*International Journal of High Performance Computing Applications*, 2002, to appear.

[9] S. Bhattacharjee, "A Dynamic Energy Efficient Multi Hop Routing Technique Using Energy Aware Clustering In Wireless Sensor Network "*Electronics Computer Technology (ICECT), 3rd International Conference* on 2011, (Volume:5)

[10] Ashim Kumar Ghosh, Anupam Kumar Bairagi , "Energy Efficient Zone Division Multihop Hierarchical Clustering Algorithm for Load Balancing in Wireless Sensor Network",*International Journal of Advanced Computer Science and Applications(IJACSA)*,Vol.2 ,No 12.

[11] Lin SHEN and XiangquanSHI ," A Location Based Clustering Algorithm for Wireless Sensor Networks" , *International Journal of Intelligent Control And Systems*, Vol. 13, No. 3, September 2008.

DOI 10.17148/IJARCCE.2015.41267