World Wide Journal of Multidisciplinary Research and Development

World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(7): 63-67
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Narpreet Kaur
Department of Computer
Engineering Guru Kashi
University Talwandi Sabo
Bathinda, Punjab, India

Jaspreet Kaur
Department of Computer
Engineering Guru Kashi
University Talwandi Sabo
Bathinda, Punjab, India

Correspondence:
Narpreet Kaur
Department of Computer
Engineering Guru Kashi
University Talwandi Sabo
Bathinda, Punjab, India

Detection and Prevention of Wormhole Attack using AFDAN protocol in MANET

Narpreet Kaur, Jaspreet Kaur

Abstract

Nodes in MANET are powered by limited batteries and their lifetime is usually less as compared to other networks such as mobile ad hoc networks. In such kind of networks, the nodes must work for longer duration of time because the replacement of the batteries is very costly affair. Since these nodes communicate wirelessly with each other, these nodes are susceptible to various kinds of security attacks. While most of the attacks have the false intention of capturing the packets and information from the network, the malicious nodes tend to drop the packets being routed towards them. It is the special arrangement where any path which has more packet drop rate will be considered as the path having attacker node. Any new path which has those attacker nodes in the intermediate list will be avoided. So that network performance can be avoided to be downgraded. In proposed technique all the performance parameters like throughput, end to end delay, success rate and packet Delivery ratio has shown the improvement.

Keywords: AFDN, SAODV, MAODV.

Introduction

MANET

MANET is a communication network formed by collection of various Mobile nodes. It refers to extremely distributed network of small, portable wireless nodes that are distributed in huge numbers to monitor the environment or system to supervise numerous characteristics like sound, temperature, voltage, pressure, pollutant levels etc. [1]. MANET is an ad-hoc network as it forms temporary network without infrastructure. It consists of transmitter and receiver nodes. These MANET s are cheap, low-power and have tremendous variety of applications.

MANET s have appeared as rising space in recent years due to advancement in Micro Electro-Mechanical Systems (MEMS) technology [2]. MANET s has leaded the development of small, cheap, lightweight, portable Mobile nodes with self-contained batteries which can accept input from an attached Mobile. This remote Mobile s has the ability to communicate with neighboring Mobile s and can share the information with each other. These Mobile nodes can also be deployed in harsh environmental conditions. It can sense or collect information from limited area of environment and has constrained battery, energy and computational capability. MANET s provides feasible solutions for a tremendous variety of applications such as medical monitoring, home security, traffic monitoring etc.

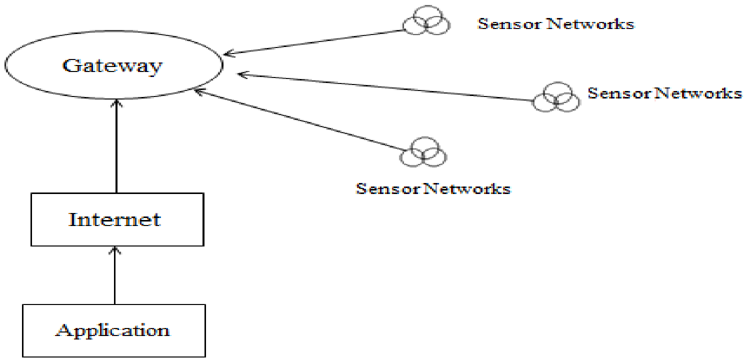


Fig. 1: MANET

MANETs were initially developed to meet the military and country security applications most importantly like battlefield surveillance. But with time, MANETs have also made a place into civilian application areas. With regards to ubiquitous computing, MANETs can be used to perform ubiquitous information sensing, storing, and provide content delivering services.

There are two types of MANET s, unstructured Mobile network and structured Mobile network. Unstructured network is a decentralized network of large number of sensing nodes leading to difficult maintenance of network and structured network has pre-planned deployment of few and scarcely distributed nodes leading to low network maintenance. The major components of a normal MANET Mobile node are a microcontroller, memory, transceiver, power source and one or more Mobile s to detect the physical phenomena. The structure of the Mobile node is generally divided into four major parts: sensing module, processing unit, communication unit and power unit. A Mobile node sends the information regarding physical phenomenon to the sink which has bigger memory and processing power. Depending on the application scenario, sometimes extra hardware is added in the Mobile nodes and a deployment strategy is devised.

Wormhole Attacks

Based on routing in Mobile networks Wormhole Attack s are considered as first class attacks in MANET. In MANET node to node data transmission is carried out by well-defined routing protocol. Wormhole Attack occurs in the network in the sense, any node in the network which is affected or infected and this node’s behavior is abruptly changing for the network, this node is called malicious node. Presence of adversary node will result in more energy consumption at each and every node. Wormhole Attack is case of denial of service attack and it is a resource (energy) depletion attack. They are called Wormhole Attack s because they drain battery power from Mobile nodes. They do not attack single node but they disrupt the entire system. Wormhole Attack can be defined as creating and sending messages that causes much more energy consumption by the network than caused by an honest node in transmitting a message of identical size and hence leading to battery drainage of nodes. These attacks do not flood network with a huge amount of data but they transmit or send small data to achieve highest depletion of battery power. Power of attack is measured by Raito of network energy in non-malignant case to network energy in malignant case. Safety from Wormhole Attack s implies that this ratio is 1. There are mainly two types of Wormhole Attack s:

Wormhole Attack S ON AODV

AODV that is Ad-hoc on demand routing protocol is a reactive protocol that preserves routes only between nodes that need to interconnect for communication. It uses on-demand methodology for discovering routes. Route table with next hop is used as routing mechanism. It supports multi-hop wireless network and is loop free. AODV initiates route discovery process when a source needs to send data packets. Routing message contain information only about source and destination it do not contain information of entire routing path. Each node in the network has its own routing table, storing node id and energy level of each node. It works on threshold energy of a node if energy of forwarding node is greater than threshold energy take it as next node otherwise broadcast the RREQ message in order to repair or find other route to reach destination. When a node needs to send packet it broadcasts a route request message to its neighbors initiating the route finding process. Each node that receives the broadcast sets reverse route to source, when the intended destination receive RREQ it generates RREP to source. When the source receives RREP it creates routes to destination and start sending packets. RERR messages are used to apprize any failure or link breakage in active path. When intermediate node detects route break it will send Route Repair (R_R) message back to pre – hope node and after sending Route repair (R_R) message it will broadcast RREQ message to repair route. If route cannot be repaired in given time than it will send Route Repair Failure (RR_F) message back to pre-hop nodes, if node repairs the route within given time that it will send Route Repair OK (RR_OK) message to its pre-hop node and the node will start sending all the waiting data. Depicting Route Invalidation is shown in below figure in this there are five nodes A, B, C, D, E and data goes from A to E via nodes B, C, D and the intermediate node C sense the link breakage it stores all data in its cache, then C sends Route Repairing message to the previous node i.e. B. After this C broadcasts Route Request message in order to repair break route. If C is not able to repair the route in certain amount of time, C sends Route Repair failure message to B and sends all data packets that are stored in its cache back to B and if C repairs route in time then it sends Route Repair OK message to B. Once node B receives Route Repairing message it caches all the data packets it receives from node A.

If node receives Route Repair Failure message from node i.e. break node, B sends Route Repair message to the pre-hop node and continues the same process. If node B receives Route Repair OK message it means that link has been repaired by C and start sending all the waiting packets to node B.

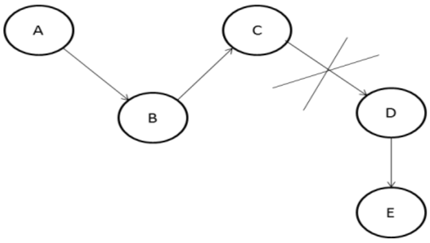


Fig. 2: Depicting Route Invalidation

Literature Survey

Parmar Amish et al (2016): Unique characteristics like limited bandwidth, limited battery power and dynamic topology makes Wireless sensor network (MANET) vulnerable to many kinds of attacks. Therefore interest in research of security in MANET has been increasing since last several years. Infrastructure less and self-governing nature of MANET is challenging issue in terms of security. Wormhole attack is one of the severe attack in wireless sensor network. In this paper, the techniques dealing with wormhole attack in MANET are surveyed and a method is proposed for detection and prevention of wormhole attack. AOMDV (Ad hoc On demand Multipath Distance Vector) routing protocol is incorporated into these method which is based on RTT (Round Trip Time) mechanism and other characteristics of wormhole attack. As compared to other solution shown in literature, proposed approach looks very promising. NS2 simulator is used to perform all simulation [1].

Haroun Benkaouha et al (2015): In this paper, they deal with failure detection in distributed systems under mobile environment constraints. For this effect, we propose a new protocol, called AFDAN (Accurate Fault Detection Protocol for Ad hoc Network), that is in charge of monitoring the distributed application against any node failure. The simulation results of our protocol show good performances in terms of accuracy and message overhead comparing to other protocols dedicated for MANETs[2].

Raksha Upadhyay et al(2015): Wireless network with a merit of sensing and processing information is known as wireless sensor network (MANET). It consists of small sensor nodes with transducer, battery, microprocessor along with storage media. It is economical and simple solution for a variety of applications. Open nature of MANET leads it to defenseless for various security threats. Several security attacks black hole, wormhole attack, DDOS attack etc. are possible to compromise the information and sensor node in network. Distributed Denial of Service (DDOS) attack is such kind of attack which aims to disrupt the network by draining resource capability. Attacker not only sends worthless messages to increase network traffic but also degrades the life of node and network[3].

Aparna U. Chaudhary et al(2015): Wireless sensor networks are the most popular network now days. It has diverse field of application which is prone to the security threats. There is fast increment in threats of attack that creates terrible problems in the network. Black hole attack is one of the security threats, in which a malicious node is occurred, which absorbs all of the data packets towards itself. That's why all data packets are dropped in that network which result in misbehaving as well as damaged node interface. For such attacks there are various types of schemes to defend over them. In this paper, we review some research paper based on black hole attack, their detection and prevention schemes, security challenges, routing protocols etc. also we discuss about Black hole attack and their types[4].

Algorithm

Step1: A network with different mobile nodes is setup. One node will works as source node and one node will works as destination node.

Step2: Send the route request to the neighbor node for identifying the destination.

Step3 Receive the route replies.

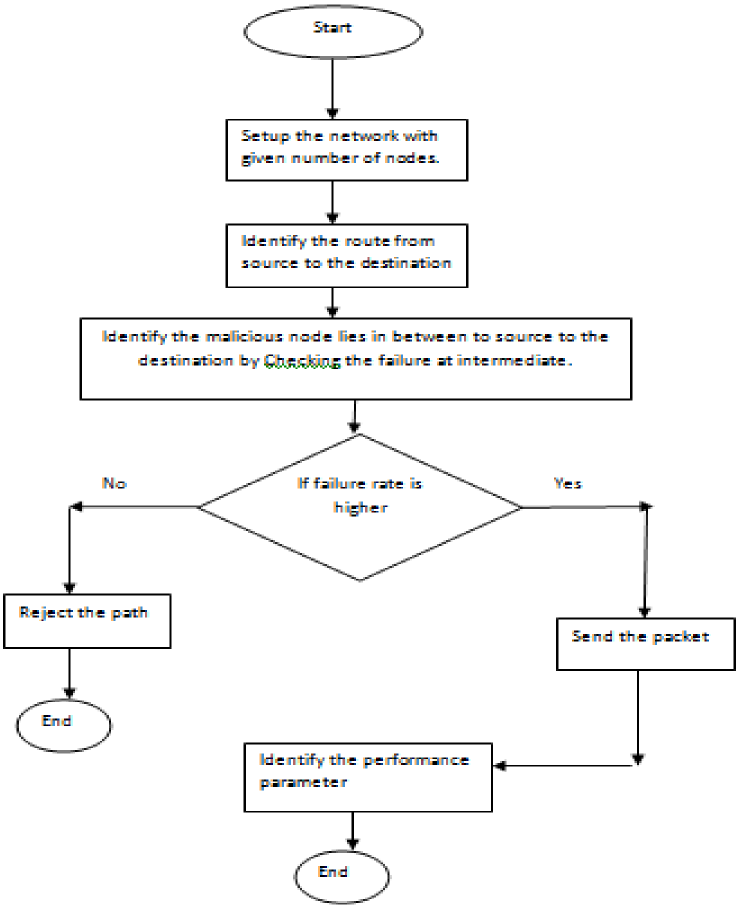
Step4: Send the hash value from the source nodes to the neighbors which are in the intermediate node list. If intermediate node has higher failure rate then the node will be considered malicious, else it will be declared legitimate.

Step5: Send the data packets on to the route which consists of legitimate nodes.

Step6: Check the network performance under different parameters like Throughput, End to End delay, Packet Delivery Ratio, Success rate.

Step7: Compare the performance on both with and without the attack.

Flow Chart


Start
Setup the network with given number of nodes.
Identify the route from source to the destination
Identify the malicious node lies in between to source to the destination by Checking the failure at intermediate.
If failure rate is higher
No
Yes
Reject the path
End
Send the packet
Identify the performance parameter
End

Simulation Setup

Parameter	Value
No. of Nodes	50
Protocol	AODV
Communication protocol	TCP,UDP
Application	CBR,FTP
Delay	1ms.
Simulation time	100

Table 1.1

This simulation setup includes basic network settings. Such that in NS2 the network can function. This network simulation shows the network in simulated way.

Problem Definition

In current research they have used the multiple path technique to identify the malicious node detection technique. Infrastructure less and self-governing nature of WSN is challenging issue in terms of security. Wormhole attack is one of the severe attack in wireless sensor network. In this research,the techniques dealing with wormhole attack in WSN are surveyed and a method is proposed for detection and prevention of wormhole attack. AOMDV (Ad hoc On demand Multipath Distance Vector) routing protocol is incorporated into these method which is based on RTT (Round Trip Time) mechanism and other characteristics of wormhole attack. This type of technique has higher vulnerability of end to end delay. Because large amount of time will be required for transmitting the false packet and then performing the calculation at the source node. Also there requires larger buffer space for storing the multiple path at the source nodes. So that once the best path will be failed, alternative route will be taken for transmitting the frames.

Objectives

1. To build a network based on wireless sensor network for given no. of nodes.
2. To implements the algorithm based on multiple path routing from source to the destination.
3. To Implements the algorithm based on AFDAN for warm hole identification from MANET.
4. To identify the various performance parameters from new builded network based on AFDAN.

Performance Parameters

a. Throughput: it is the amount of packet sent per unit interval of time. These successful packets that has been arrived at the destination.

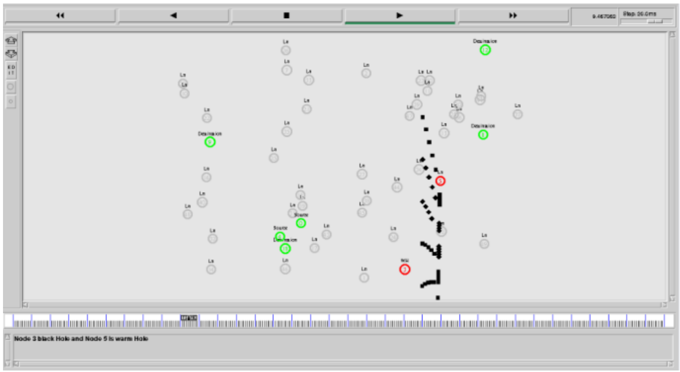
b. End to End delay: it is the difference of end time and start time. Start time is at what time packet has been sent. And received time if the time at which packet has been received.

c. Packet Delivery Ratio: it is the ration of packet sent versus packet dropped. Packets can be dropped due to the congestion or attacker node or with some other problem.

d. Success Rate: it is the measure of success rate. that means how many packets has been sent and how many packets has been received.

Results and Discussions

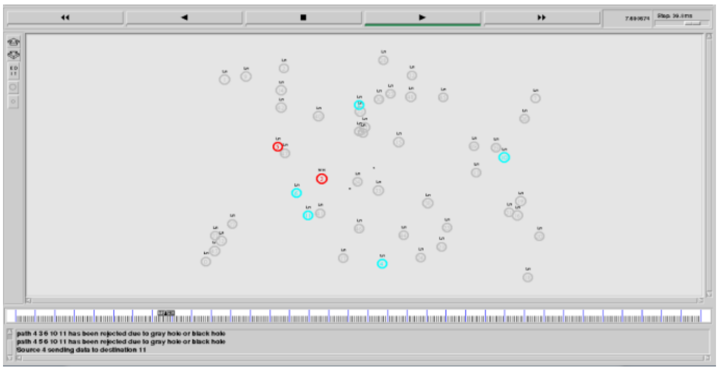
Nam simulation for network with attack.



Node 3 black Hole and Node 5 is warm Hole

Fig. 3

This nam simulation shows the attacker node. Where any packet arrives at this node all the packets will be dropped. This will deteriorate the performance of the network.
Nam simulation for network without attack**.**

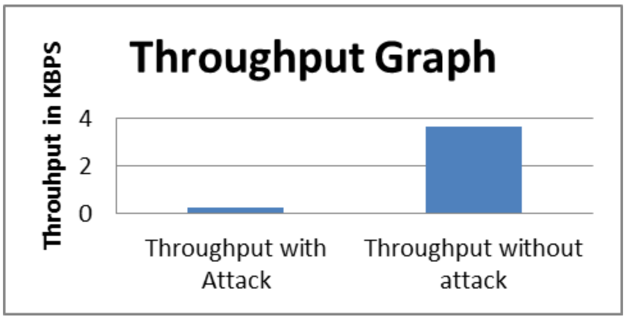


path 4 3 6 10 11 has been rejected due to gray hole or black hole
path 4 5 6 10 11 has been rejected due to gray hole or black hole
Source 4 sending data to destination 11

Fig. 4

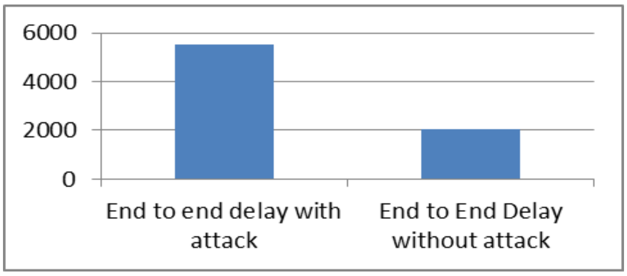
This network shows that the attacker node has been identified. Now when in any path these attacker will be encountered the path will be left. That path will be adopted which has no attacker node.

Throughput graph for network with and without attack

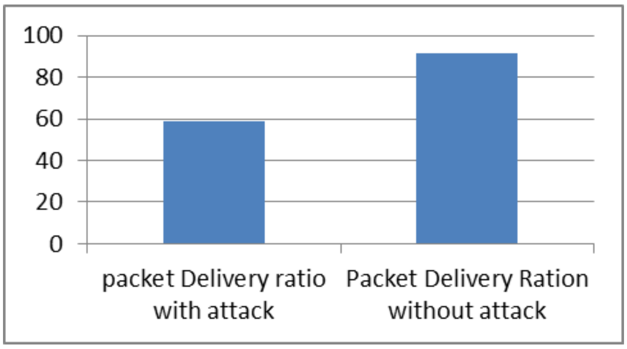


Graph 1

End to end delay graph for network with and without attack

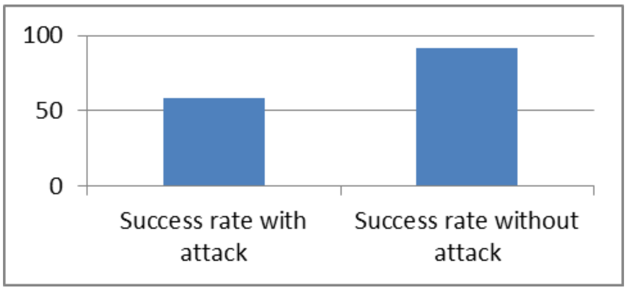


Packet delivery ratio graph for network with and without attack.



Graph 1.3

Success rate graph for network with attack and without attack



Graph 1.4

Above table shows that the network performance on the basis of all the factors has shown the improvement. This means AODV has really improved to AFDN. As AFDN Where any attacker node cannot destroy the network performance.

Conclusion and Future Work

MANET is the mobile ad-hoc network. It is infrastructure less network. There is no central controller which can control the network performance and secure the network from various kinds of attacks. There requires the special arrangement in the protocol so that the attacker node can be identified and removed. It is the special arrangement where any path which has more packet drop rate will be considered as the path having attacker node. Any new path which has those attacker nodes in the intermediate list will be avoided. So that network performance can be avoided to be downgraded. In proposed technique all the performance parameters like throughput, end to end delay, success rate and packet Delivery ratio has shown the improvement. In future work further will be extended so that the performance can be further enhanced.

References

1. Parmar Amish, V.B.Vaghela," Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol", Procedia Computer Science 79 (2016) 700 – 707
2. Haroun Benkaouha † Abdelkrim Adelli †, Nadjib Badache † Jalel Ben-Othman‡, and Lynda Mokdad," AFDAN: Accurate Failure Detection protocol for MANETs", 978-1-4799-5344-8/15
3. Lijun Qiana,_, Ning Songa, Xiangfang Lib.," Detection of wormhole attacks in multi-path routed wireless ad hoc networks: A statistical analysis approach", Computer Applications 30 (2007) 308–330
4. Raksha Upadhyay, Salman Khan, Harendra Tripathi, Uma Rathore Bhatt," Detection and Prevention of DDOS Attack in WSN for AODV and DSR using Battery Drain", 2015 Intl. Conference on Computing and Network Communications (CoCoNet'15), Dec. 16-19, 2015, Trivandrum, India
5. Aparna U. Chaudhary, Prof. Priti A. Khodke, Prof. A. U. Chaudhari," A Review on Black Hole Attack Detection and Prevention Schemes in Wireless Sensor Network", Volume 5, Issue 10, October-2015
6. Swaijit Kaushal 1, Reena Aggarwal," Avoidance of Wormhole Attack by using Delphi method", Volume: 02 Issue: 07 | Oct-2015
7. Guowei Wu1, Xiaojie Chen1, Lin Yao1, Youngjun Lee2, and Kangbin Yim2," An Efficient Wormhole Attack Detection Method in Wireless Sensor Networks", Computer Science and Information Systems 11(3):1127–1141
8. Sonal Shrivastava, 2Chetan Agrawal & 3Anurag Jain," An IDS scheme against Black hole Attack to Secure AOMDV Routing in MANET",vol3 issue 5 2015
9. M.U Bhatti D. Conan, D´etection de partition pour la gestion de groups en environnement mobile. UbiMob ACM. 2005- p 65-72,
10. E. Jim´enez, S. Ar´evale, A. Fern´andez. Implementing unreliable failure detectors with unknown membership. Join 2006.
11. P. Sens L Arantes M. Bouillaguet V. Simon and F. Greve. An Unreliable Failure Detector for Unknown and Mobile Networks. 12th ICPDS, Luxor, Egypt, Dec 15-18, 2008. p 555–559, 2008.