ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Securing WMN by Mitigating Insider Selective Forwarding Attack through FADE

Rachna Beniwal[1], Nisha Pandey[2],

M.Tech Student, Dept. of CSE & Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India [1]

Asst. Prof, Dept. of CSE & Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India. [2]

ABSTRACT: Wireless mesh networks (WMNs) are evolving as a solution for large scale high speed internet access via their self-configuring, scalability and low cost. But in comparison of wired networks, WMNs are highly prone to various security attacks because of its distributed architecture, open medium nature and dynamic topology. This paper takes a particular kind of DoS attack known as selective forwarding attack. With this type of attack, a misbehaving mesh router just sends few packets it obtains but discards sensitive data packets. To mitigate the impact of this attack a mechanism known as FADE: Forward Assessment based Detection is followed. FADE mechanism determines the existence of attack inside the network by means of two-hop acknowledgment based monitoring and forward assessment based detection. FADE runs in three stages and examined by detecting optimal threshold values. This method is determined to offer efficient defense against the cooperative internal attackers in WMNs.

KEYWORDS: Wireless mesh network, FADE, selective forwarding attack,

I. INTRODUCTION

Wireless mesh networks (WMNs) are a multi-hop wireless communication among various nodes are dynamically self-configured and self-organized, with the network nodes automatically demonstrating an ad-hoc network and managing the mesh connectivity. WMNS are issued as a predicting concept to fulfil the challenges in wireless networks i.e. adaptability, flexibility, reconfigurable architecture etc. Wireless mesh networks (WMNs) are developing as a solution for large scale high speed internet access via their self-configuring, scalability and low cost. But in comparison of wired networks, WMNs are highly prone to various security attacks because of its distributed architecture, open medium nature and dynamic configuration. Denial of service (DoS) attacks is one of the most general kinds of attack which can occur in WMNs. DoS attacks are most general in networks which link to internet and however WMNs are primarily intended for long distance and fast internet access this kind of attacks are common in the network. The three important features of Wireless Mesh Networks (WMN) are 1) Self-healing, 2) Self-organizing, 3) Self-optimizing. This paper assumes *Infrastructure WMNs,* a kind of WMNs where the stationary mesh routers builds an infrastructure to the mesh clients that links to them. The other kinds of WMNs involve *Client WMNs* where the meshing offers peer-to-peer connectivity between the client devices. The clients performs the actual routing and other services and *Hybrid WMNs* which is an integration of both client and infrastructure WMNs, Here the mesh clients can access the internet through mesh routers or else directly meshing via other devices. The wireless mesh networks architecture can be categorized in to three main groups depending on the nodes services namely client WMNs, infrastructure/backbone WMNs and Hybrid WMNs. In infrastructure WMNs wireless mesh routers will make a mesh of self-healing, self-configuring connections among themselves. With gateway service these routers can be linked to the internet. This mechanism offers backbone for traditional clients and enables combination of WMNs with available wireless networks, via gateway/bridge services in mesh routers. In client meshing the client devices will make a mesh to perform configuration and routing functionalities as well as offering end-user applications to subscribers. In this architecture no mesh routers are represented and hence are same as the traditional ad-hoc network. Hybrid WMNs is the integration of client and infrastructure meshing and a mesh network is built between the routers and as well as the clients. Mesh clients can access the network via mesh routers as well as directly meshing with each other. Wireless mesh network in which nodes forward and obtain data by utilizing mesh network.[5] Wireless mesh network is a wireless communication between various nodes which are self configured and self organized with nodes in network and build Ad hoc that shown in figure 1.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

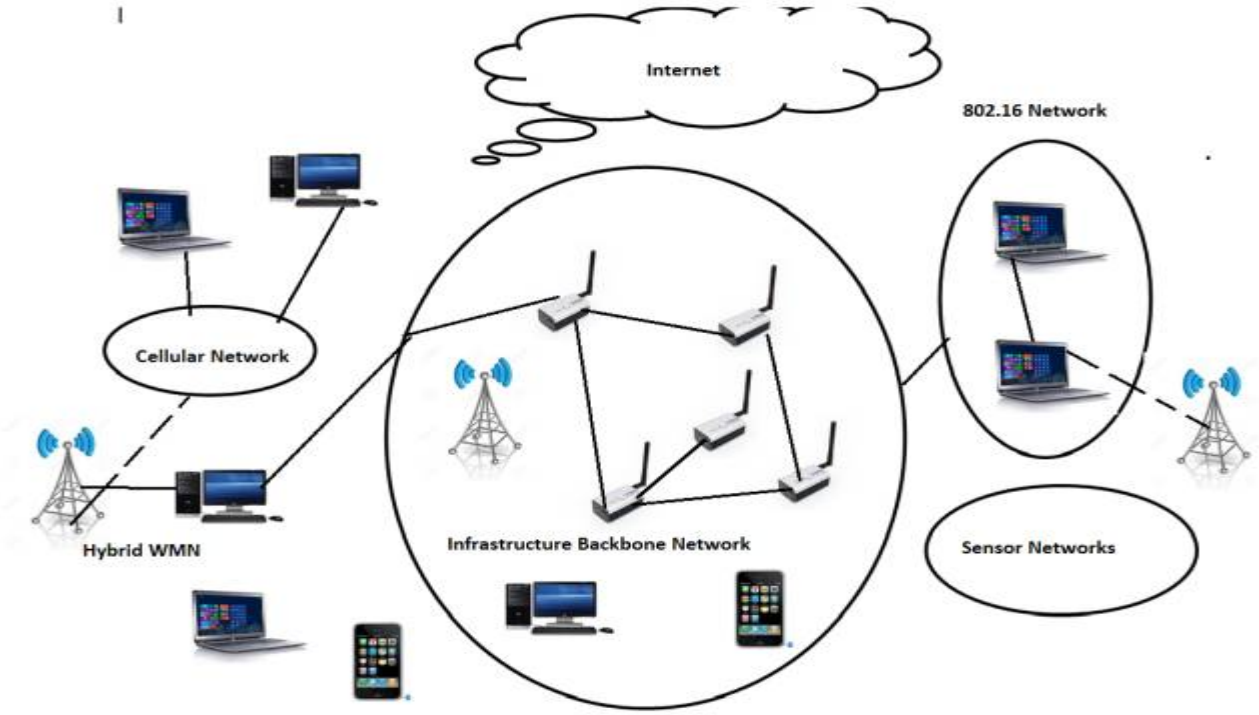

Figure: 1 Wireless mesh networks

II. LITERATURE REVIEW

Watchdog monitoring technique was proposed by Marti *et al.* [5] to detect misbehaving nodes in wireless ad hoc networks. This technique can be employed in WMN and it was the former trust technique which is the basis of several defence mechanisms. In their mechanism, every sensor node has its own watchdog that maintains and stores the behaviours of its one neighbouring hop. The watchdog method of every node saves the routing table which is about the performance bad or good of the neighbouring nodes. When the node M forwards a packet to its neighbouring node N, the watchdog of M detects whether N send the packet to the BS or not by utilizing the sensor's overhearing capability. The benefit of this type of security technique is that the principle is simple, complication is low and it adjusts to the WMN totally. But this mechanism can only solve restricted situations of harmful nodes packet discarding.

Depending on Watchdog mechanism, Yu *et al.* [1] explain various representative methods to make a trust model. In their research paper, Bayesian mechanism, Entropy mechanism, Game-theoretic mechanism, and Fuzzy approach are introduced. By the various algorithms, we change the information which comes from the watchdog mechanism to statistical data for weighing the behaviour of maintained node whether bad or good. The design of trust measurement is proposed at examining the situation of detecting a forwarding node. We expect to select the node whose all types of attributes are comprehensively correct as the adjacent-hop node.

Employing various trust models, the reputation value of a node will be distinct. When the trust model is evaluated, we should adjust a fair threshold. If a node's reputation value is less than the threshold, it will be stored as a harmful node. Furthermore, based on the WMN's trust technique, the detection of these harmful node will or will not be forward to the remaining nodes and base station in the WMN.

Harmful node may be the intersection of various routes, that is to say this type of node may broadcast more than one source node's data. It can discard the data package of one or many node between those source nodes so that the determination to this harmful node from every source node is different. Hence, this type of harmful node cannot be

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

rejected in time. Hence, a detection technique depending on neighbor nodes managing was introduced. By hearing to each other, every node considers statistics of the no. of broadcasted packets by neighbouring nodes. Then, every node computes the reputation values of its neighbouring nodes. All reputation values information will be set up for computing every node's weighted credibility. Various works [6] [7] that utilized neighbour-based mechanism have been presented for mitigating selective forwarding attacks. Lu *et al.* [7] have introduced a neighbour-based monitoring technique. In their design, every node calculates the trust value of its 1-hop neighbours depending on their various behaviour measurement and creates a trust management so that it can ensure whether a node is a harmful node or not. The advantage of this mechanism is that we can detect the caught node more quickly and accurately by various nodes
No matter how analysing the detection technique is, it always demonstrates on the condition that harmful nodes have already dropped a mass of data packets. Hence, if we wish to make confirm that the packets are broadcasted to the base station completely, we should let the packets avoid the harmful node.
B.Yu [8] introduces a mechanism to determine selective forwarding attacks depending on checkpoints. If any checkpoints node doesn't obtain enough acknowledgments, it will create warning messages to the source node, so that the determination of the selective forwarding attacks can be observed. But an apparent issue is available in this mechanism is that the nodes have to forward acknowledgments in a continuous way, which will highly increase the network cost. By the way, this mechanism can't decide whether there malicious tamper action available.
Jiang [9] introduces a mechanism to determine selective forwarding attacks, which depend on the trust level and packet loss. After networking configuration being demonstrated, when sensing data is transmitted on the route, the intermediary nodes determine and count the no. of the packets they obtain and forward, and inform the statistical results to the Base station; with respect to these data, the BS computes the trust level of nodes and measure the packet drop, so that it can detect whether this node is an active attacking node
Yu and Xiao in [10], introduced a technique which utilizes a multi-hop acknowledgment mechanism to launch alarms by receiving replies from intermediary nodes. Every node in the forwarding path is in charge of determining harmful nodes. If an intermediary node determines a node as harmful in its upstream/downstream, then it will forward an alarm packet to the base station/source node via multi-hops
Sophia Kaplantzis et al [11] introduced a centralized intrusion detection technique that utilizes only two characteristics to determine selective forwarding and black hole depending on Support Vector Machines (SVMs) and sliding windows. This intrusion detection is operated in the BS and thus the sensor nodes utilize no energy to support this extra security characteristic. From this they conclude that the system can determine selective forwarding attacks and black hole attacks with high accuracy without exhausting the nodes of their energy.
Brown and Xiaojiang [12] have introduced a technique to determine selective forwarding utilizing a Heterogeneous Sensor Network (HSN) model. The HSN contains powerful high-end sensors (H-sensors) and large no. of low-end sensors (L sensors). After deploying sensors, a cluster formation occurs with H-sensor as cluster head.
Xin, etal. introduced [13] a light weight defence technique against selective forwarding attack which utilizes neighbour nodes as monitor nodes. The neighbouring nodes (monitoring nodes) monitor the transmission of packet loss and re-forward the lost packets. They employed a hexagonal WSN mesh configuration.
Zurina Mohd Hanapi et al [14] introduced the dynamic window stateless routing protocol DWSIGF that is resilience to selective forwarding and black hole attack caused by the CTS rushing attack. Even without embedding any security technique inside the routing protocol, the dynamic window protected implicit geographic forwarding (DWSIGF) however promise a good defence against black hole attack with good performance of network.
Riaz Ahmed Shaikh et al [15] introduced two new identity, location privacy and route algorithms and data privacy method that addresses the challenging issues because of the constraints imposed by the sensor networks, sensor nodes and QoS problems.

III. PROBLEM DESCRIPTION

When linked to internet, the mesh routers build backbone to offer functionality to mesh clients (infrastructure WMNs). These mesh routers are less mobile and acts as gateways in several cases. An outside attacker may adjust a mesh router within the network and obtain access to sensitive data i.e. private, public and group keys and guides the router to perform in a malicious way. Mostly routing protocols intended for WMNs such as Hybrid Wireless Mesh Protocol (HWMP) and Ad hoc On-Demand Distance Vector (AODV) consider that all nodes reliably send packets. The protocols utilized in mesh networks do not consist self-contained security measures for determining attacker nodes. In

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

some situations a single mesh router in the packet sending path may be adjusted such as standalone attacker can be easily determined by the acknowledgment forwarded by the other trusted routers within the network.
This paper covers colluding attackers such as two or more routers within the network may be adjusted by the outside attacker. The Figure1 depicts the network model operating selective forwarding attack [21]. The network has a source that creates the information that must be propagated to the destination through a gateway that links the network to the

IV. SELECTIVE FORWARDING ATTACK

The Selective Forwarding attack, a particular case of DoS attack, was first explained by Karlof [1] as "an attack where the harmful node deny to send particular messages and simply discards them assuring they are not forwarded any further." It is normally considered that the intermediary nodes, in multi-hop sensor networks, playing role in the communication mechanism between the sink and the source, reliably send the messages they obtain from the other nodes [1]. In the Selective forwarding attack, also called Gray hole attack, the adjusted node tries to interrupt the normal communication mechanism by selectively dropping the particular packets while sending the others. The adversary may select to discard the packets producing from the specific node or a group of nodes, hence leading to the DoS for that node(s) or the packets of a specific type, for instance, packet reporting the tank coordinates in battlefield. The selective forwarding attack can be established as inside attack by adjusting a legitimate node within the network to discard the subset of packets while sending the others. To be more efficient, the adversary attempts to position itself on the real data flow path between the two communicating nodes as this will support to obtain more traffic. Due to the restricted transmission range, sensor networks sends the packets to the BS in multi-hop way and while being forwarded to the BS packets may be discarded due to congestion, collision or other network issues. The selective forwarding attack exploits these network issues and hence becomes more complex to determine.

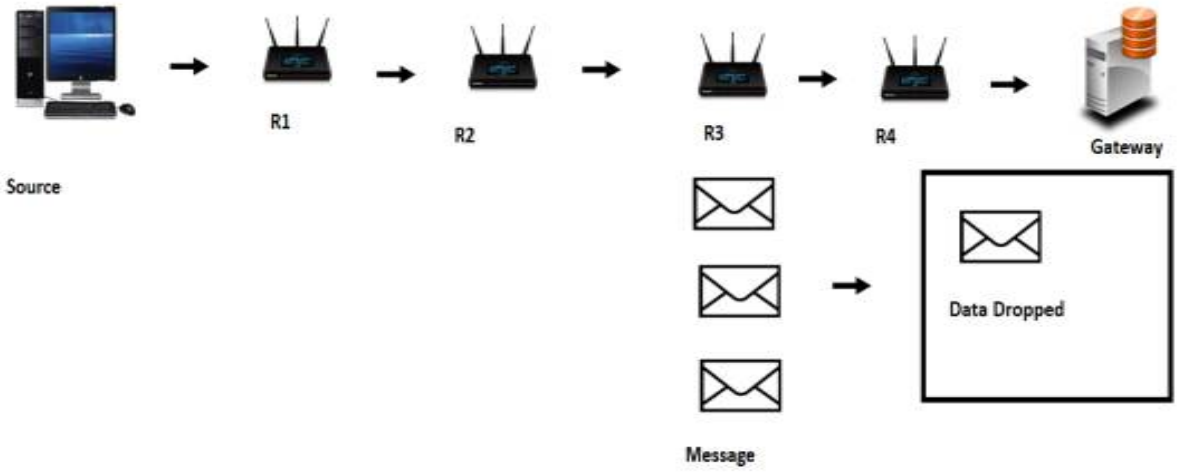

Figure 2: Selective Forwarding attack

V. PROPOSED SYSTEM

5.1 Preview: The FADE (Forward Assessment based Detection) mechanism is utilized to determine the existence of colluding attackers in the WMNs. This mechanism has performance same as CAD (Channel Aware Detection) with an extra benefit of determining collaborative attackers in the network. FADE mechanism follows two techniques namely monitoring and multidimensional assessment.
FADE mechanism apart from determining colluding attackers it also determines various attacks i.e. counterfeit attack and malicious accusation attack. FADE is a non-cryptographic technique and operate in different underlying protocols. It must be confirmed that all the mesh nodes must be authorized utilizing the link layer security protocols thus securing

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

the network against external attackers from overhearing the message. Also the messages transferred are further secured by key management mechanisms. However link layer security is ensured by the protected protocols and several encryption standards FADE mechanism is capable of determining the attackers decreasing the network layer performance. Hence FADE mechanism is utilized to differentiate the trusted nodes from the inside attackers in the network.

Monitoring: The nature of both downstream and upstream nodes is assessed by two hop acknowledgement technique. The service of an intermediary node in the network is examined by the opinion of its both downstream and upstream nodes. The monitoring mechanism can determine standalone attackers in the network. The monitoring mechanism utilizes acknowledgement from both downstream and upstream nodes to determine the loyalty of a specific node within the network.

Forwarding assessment based detection of attacks*:* By following multidimensional assessment, the normal nature of a node can be detected by utilizing the opinion of both downstream and upstream nodes. By integrating the opinion of end-to-end assessment and downstream assessment, collaborative grey hole attack can be determined. CAD technique which utilizes only monitoring is an efficient Way of determining only standalone attackers in the network. When it comes to colluding attackers, CAD mechanism is not applicable, thus FADE utilizes an extra multidimensional assessment mechanism.

5.2 Assumptions: It is considered that the mesh nodes have no energy constraint and all the mesh nodes are considered to be stationary, making a mesh backbone for infrastructure WMNs. The dynamic configuration, self-organizing and decentralized nature of WMNs builds it prone to attacks. The following consideration is taken in the introduced technique. The network is assumed to be strongly linked. There happen a no. of paths between the source and destination. The protocol utilizes the best path between the sources to destination node for the packet transmission. The mesh routers are highly authorized and the secure encryption mechanism is followed. All the network routers have enough memory to store the packets obtained.

VI. SIMULATION RESULTS

The simulation is done in network simulator ns2 (v2.33) with a network consisting an average of 45 static nodes (numbered 0 to 44). ns2 utilize TCL language for generating simulation scenario file (for instance, sample.tcl). Transmission time, Network topology utilizing protocols is described in scenario file. The visualization tools are X graph and nam (network animator) fie. The NAM file is a packet level animator well survived by ns2. The X graph offers the results of simulation in the form of graph. The routing protocol utilized in DSR. Figure 3 demonstrating Route Between Source node To Destination node.

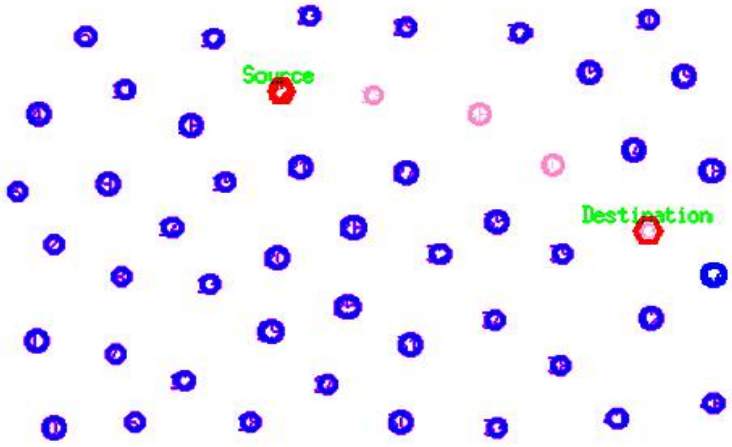

Figure 3: Establishing Route between Source To Destination

The figure 3 represents the route establishment between source node to destination node takes place and normal data transmission occurs without the availability of attacker.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

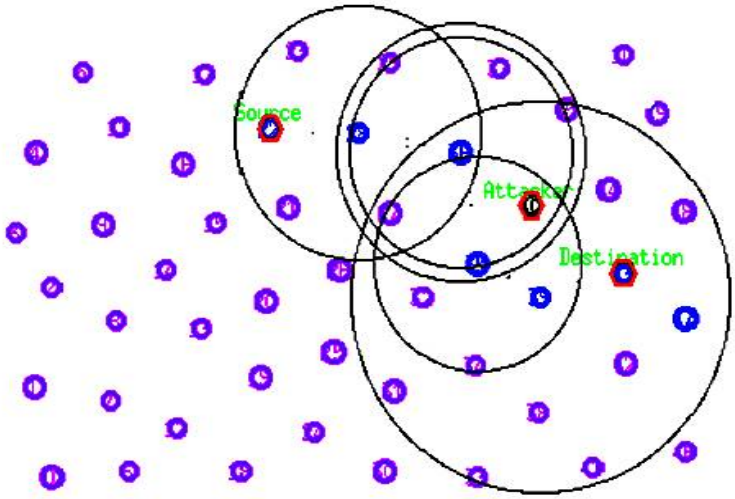

Figure 4: Packet Transmission In The Presence Of Attacker

The figure 4 represents network with attacker in the data transmission path. The attacker cause packet drop and FADE mechanism running in the underlying protocol determines the availability of attacker in the network by the above mentioned mechanisms.

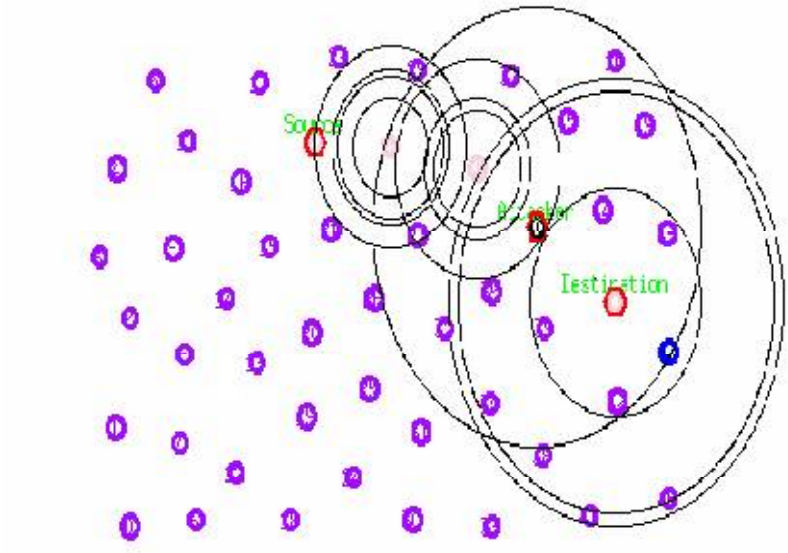

Figure 5: Rerouting In A New Path After Detection Of Attacker

The fig 5 shows the rerouting of the path by eliminating the attacker from the network.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

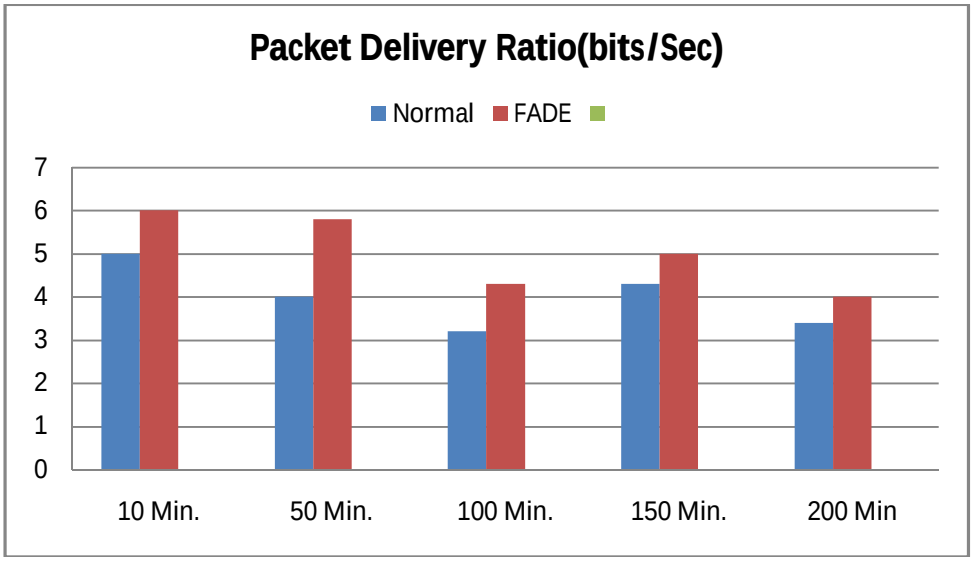

Figure: 6 Packet Delivery Ratios in WMN

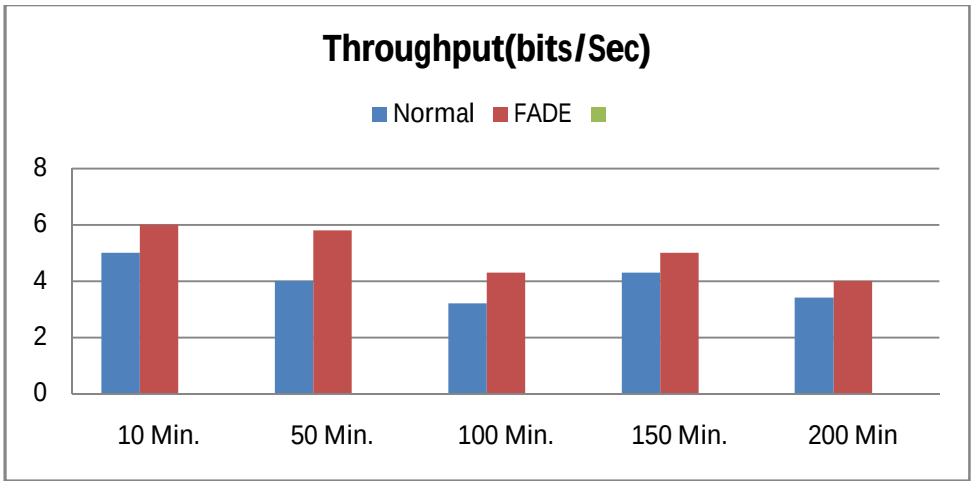

Figure: 7 Throughputs in WMN

The FADE scheme offers high throughput and packet delivery ratio that shown in figure 6 and 7. Because FADE mechanism utilizes both multidimensional assessment and monitoring techniques to determine the colluding attackers within the network. Apart from only determination of attacker in the routing path, this mechanism also re-sends the packets in a new path removing the attacker from the data forwarding route.

VII. CONCLUSION AND FUTURE WORK

WMNs are employed for military applications where protected routing of information is the major need. The FADE mechanism utilizes both multidimensional assessment and monitoring techniques to determine the colluding attackers within the network. Apart from only determination of attacker in the routing path, this mechanism also re-sends the packets in a new path removing the attacker from the data forwarding route. This mechanism is very efficient in determining the attacker within the network, thus a secure routing concept may be followed in resolving and

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

eliminating the attacker from the network In future I have plan to build the threshold values dynamic in the existence of normal loses because of wireless channel and MAC layer collisions and to work on the attacks when the attack routers collude together. However routers in WMNs work in an entirely wireless atmosphere the packet can be dropped because of several factors. So finding a suitable threshold value for determining the gray hole attack in real environment is really hard. Wireless mesh networks is having an open architecture and more vulnerable to Denial of Service attacks because of its usage in broadband internet access. Hence more research work has to be performed to decrease the Denial of Service attacks and enhance the network.

REFERENCES

[1]H. Lee, V. Mashhad, and D. Cox, "Time-driven simulation of large wireless networks with parallel processing," IEEE Communications Magazine, vol. 47, no. 3, pp. 158-165, Mar. 2009.
[2] H. Lee and Zu Li, "Simulation of mobile cellular systems with integrated resource allocation and adaptive antennas," Proc. of IEEE Wireless Communications and Networking Conference (WCNC), pp. 3210-3215, Mar. 2007
[3] A. Goldsmith and L. Greenstein, "A measurement-based model for predicting coverage areas of urban microcells," IEEE Journal on Selected Areas in Communications, vol. 11, no. 7, pp. 1013-1023, Sep. 1993.
[4] D. Cox, R. Murray, and A. Norris, "800 MHz attenuation measured in and around suburban houses," AT & T Bell Laboratories Technical Journal, vol. 63, no. 6, pp. 921-954, Jul./Aug. 1984.
[5] Z. Tang and J. Garcia-Luna-Aceves, "A protocol for topology-dependent transmission scheduling in wireless networks," Proc. of IEEE Wireless Communications and Networking Conference (WCNC), pp. 1333-1337, Sep. 1999
[6] C. Zhu and M. Corson," Reservation protocol for mobile ad hoc networks," Wireless Networks, vol. 7, no. 4, pp. 371-384, Jul. 2001.
[7] W. Smith, "Urban propagation modeling for wireless systems," Ph.D. dissertation, Stanford University, Stanford, CA, USA, Feb. 2004
[8] M. Feuerstein et al., "Path loss, delay spread, and outage models as functions of antenna height for microcellular system design," IEEE Transactions on Vehicular Technology, vol. 43, no. 3, pp. 487-498, Aug. 1994.
[9] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liangmin. "Lightweight defense scheme against selective forwarding attacks in wireless sensor networks" pages 226 –232, Oct. 2009
[10] C. Intanagonwirat, R. Govindan and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks," in 6th Annual Conf. on Mobile Computing and Networking, pp. 56-67. Aug. 2000.
[11] B. Karp and H. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," in 6th Annual Conf. on Mobile Computing and Networking, pp. 243-254, Aug. 2000.
[12] Wazir Zada Khan et.al "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks" in I.J. Computer Network and Information Security, pp.1-10, Aug-2012
[13] Anthony Wood, John A. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, 35(10):54-62, October 2002.
[14] B Yu, B Xiao. "Detecting selective forwarding attacks in wireless sensor networks". In: Proe. of the 20th International Parallel and Distributed Processing Symposium, RhodesIsland, Greeee,pp.1218- 1230, 2000
[15] Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, November, pp. 1-4, 2006.