INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 3 ISSUE 1 –JANUARY 2015 - ISSN: 2349 - 9303

Mitigation of Colluding Selective Forwarding Attack in WMNs using FADE

C.Gayathri
M.E – Communication systems
M.Kumarasamy College of Engineering , Karur
gayathrichandrasekar92@gmail.com

Dr.V.Kavitha
Professor & Head - ECE
M.Kumarasamy College of Engineering , Karur
emiroece@gmail.com

ABSTRACT - Wireless Mesh Networks (WMNs) have emerged as a promising technology because of their wide range of applications. Wireless mesh networks wireless mesh networks (WMNs) are dynamically self – organizing, self – configuring, self – healing with nodes in the network automatically establishing an adHoc network and maintaining mesh connectivity. Because of their fast connectivity wireless mesh networks (WMNs) is widely used in military applications. Security is the major constrain in wireless mesh networks (WMNs). This paper considers a special type of DoS attack called selective forwarding attack or greyhole attack. With such an attack, a misbehaving mesh router just forwards few packets it receives but drops sensitive data packets. To mitigate the effect of such attack an approach called FADE : Forward Assessment based Detection is adopted. FADE scheme detects the presence of attack inside the network by means of two-hop acknowledgment based monitoring and forward assessment based detection. FADE operates in three phases and analyzed by determining optimal threshold values. This approach is found to provide effective defense against the collaborative internal attackers in WMNs.

Key words: Wireless Mesh Networks (WMNs), Colluding, FADE, Selective forwarding attacks, security.

1 INTRODUCTION

Wireless mesh networks (WMNs) are a multi-hop wireless communication among different nodes are dynamically self-organized and self-configured, with the nodes in the network automatically establishing an ad-hoc network and maintaining the mesh connectivity. WMNS are emerged as a promising concept to meet the challenges in wireless networks such as flexibility, adaptability, reconfigurable architecture etc. Wireless mesh networks (WMNs) are emerging as a solution for large scale high speed internet access through their scalability, self configuring and low cost. But as compared to wired networks, WMNs are largely prone to different security attacks due to its open medium nature, distributed architecture and dynamic topology. Denial of service (DoS) attacks is one of the most common types of attack which is possible in WMNs. DoS attacks are most common in networks which connect to internet and since WMNs are mainly designed for fast and long distance internet access this type of attacks are common in the network. The three main characteristics of Wireless Mesh Networks are 1) Self-organizing, 2) Self-healing, 3) Self-optimizing.

This paper considers *Infrastructure WMNs*, a type of WMNs where the static mesh routers forms an infrastructure to the mesh clients that connects to them. The other types of WMNs include *Client WMNs* where the meshing provides peer-to-peer connectivity among the client devices.

The clients performs the actual routing and other functionalities and *Hybrid WMNs* which is a combination of both infrastructure and client WMNs, Here the mesh clients can access the internet via mesh routers or else directly meshing through other devices.

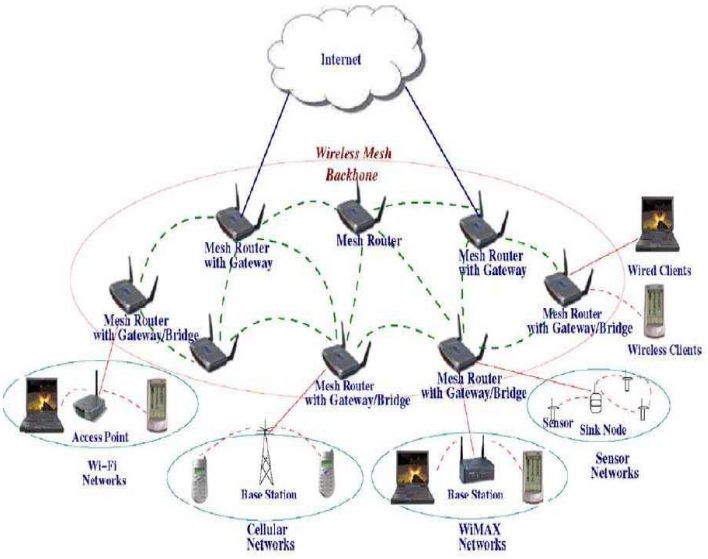

Fig 1.1. Infrastructure WMNs

The various advantages of WMNs are

1. Low Cost – Using relatively low power, commercially available radios and requiring no cabling or wires, mesh networks provide a low-cost alternative to wired or distributed RF networks.

2.Quality of Service – QoS algorithms enable transmission of multimedia traffic and video with little or no loss or latency.

3. Flexible – Mesh networks support any IP-enabled device or application.

4. Scalable – Mesh networks can quickly scale to thousands of nodes covering hundreds of miles.

5. Reliable – Each mesh node is backed up by multiple peers, providing an always-on grid of communication links.

A compromised, malicious router can silently discard data packets to degrade the network performance. In this attack, malicious nodes forward control packets normally but selectively drop data packets. The attack could lead to serious damage when sensitive data are lost. Moreover, since network traffic in a WMN aggregates at a special type of MR, called the gateway, which connects the mesh backbone with the global network. Thus, an attacker can advertise a route with the minimum cost to the gateway, then it can selectively drop data packets received from upstream MRs. While most of the existing studies on selective forwarding attacks focus on detecting stand-alone attackers based on channel overhearing, we examine a more sophisticated scenario in which multiple malicious nodes perform collaborative grey hole attacks. In addition, some security features like per-link encryption provided by render existing detection solutions that rely on channel overhearing unusable. Therefore, it is important to develop novel methods that are compatible with contemporary link layer protection schemes. In this paper, we propose a forwarding assessment based detection (FADE) scheme to address the above two challenges.

2 RELATED WORK

R. Curtmola and C. Nita-Rotaru [3] described a novel secure routing protocol called BSMR (Byzantine Resilient Secure Multicast Routing Protocol) to defend against insider attacks from colluding adversaries. Byzantine attacks includes blackhole attack , greyhole attack , wormhole attack etc. The protocol is a software-based solution and does not require additional or specialized hardware. The protocol maintains bi-directional shared multicast trees connecting multicast sources and receivers. The main operations of the protocol are route discovery, route activation and tree maintenance. The protocol fails due to higher overhead because both route request and route reply are broadcast messages.

Xiao , Yu , Gao [5] described a technique a lightweight security scheme that detects selective forwarding attacks by using a checkpoint-based acknowledgement technique.The suspect nodes are identified and localized using checkpoint selection strategy.

With this strategy, parts of intermediate nodes along a forwarding path can be randomly selected as checkpoint nodes, which are responsible for acknowledgement for each packet safely delivered to them. This checkpoint selection algorithm has two main steps: *intermediate node bootstrapping*, and *random-checkpoint-based acknowledgement*. This scheme suffers from larger overhead.

Eriksson, Faloutsos and Krishnamurthy [6] identified a secure routing protocol called Sprout, which continuously tries new routes to destination to resolve the presence of colluding attackers in the network. Sprout mitigates the various routing layer attacks even under the presence of large number of colluding attackers, by adjusting the traffic sent on each path accordingly. Sprout is a source-routed, link-state, multi-path routing protocol with a probabilistic twist. Routing is done in two stages: route generation, and route selection.

Sun , Chen and Hsiao [7] proposed a light weight and simple scheme called MDT(Multi Dataflow Topologies) to defend against selective forwarding attackers in the network which selectively drops the sensitive data information. Apart from selective forwarding attack this scheme also detects mobile jamming attack and sinkhole attacks. Here the base station divides the sensor nodes into different groups and each of these groups follows different dataflow topologies. Once the multi dataflow topology is constructed, each sensor node senses around itself and sends the information to the base station. Though one group has malicious nodes and it drops the data packets. These packets still reaches the base station through the other dataflow topologies since the sensing areas are overlapped. There is no need for the retransmission of information.

K. Ren, W. Lou, Y. Jhong [9] developed location-aware end-to-end security framework in which each node only stores a few secret keys and those secret keys are bound to the node's geographic location . In LEDS, every report is encrypted by the corresponding cell key and therefore, no nodes out of the event cell could obtain its content. Compromising many intermediate nodes will not break the confidentiality of the report. Only when a node from the event cell is compromised could the attacker obtain the contents of the corresponding reports. . The strength of LEDS comes from both its report endorsement mechanism and its forwarding mechanism. LEDS is highly robust against selective forwarding attacks as compared to the traditional one-to-one forwarding approach used by existing security designs. The scheme lags because of usage of larger resources and higher overhead.

Khalil , Saurabh Bagchi, Cristina N.-Rotaru, Ness Shroff [15] developed lightweight framework called UNMASK (**U**tilizing **N**eighbor **M**onitoring for **A**ttacks Mitigation in Multihop Wireless **S**ensor Networ**k**s), that mitigates such attacks by isolating the malicious nodes.

UNMASK uses as a original ability of a node to oversee its neighboring nodes' communication. On top of UNMASK, a secure routing protocol called LSR is built that provides additional protection against malicious nodes by supporting multiple node-disjoint paths. UNMASK provides the following primitives - *neighbor discovery* and *one-hop source authentication*. These two primitives are then used as the building blocks for the two main modules - *local monitoring* and *local response*. The design features of LSR described below make it resilient to a large class of control attacks such as wormhole, Sybil, and rushing attacks, as well as authentication and ID spoofing attacks. Combination of UNMASK and LSR can deterministically detect and isolate nodes involved in initiation of these attacks.

Shila, Cheng, and Anjali [17] described a technique to detect standalone selective forwarding attacker in the network. The CAD approach is based on two procedures, channel estimation and traffic monitoring. The procedure of channel estimation is to estimate the normal loss rate due to bad channel quality or medium access collision. The procedure of traffic monitoring is to monitor the actual loss rate; if the monitored loss rate at certain hops exceeds the estimated loss rate, those nodes involved will be identified as attackers. , the traffic monitoring procedure at each intermediary node1 along a path monitors the behaviors of both its upstream and downstream neighbors, termed as upstream monitoring and downstream monitoring, respectively. The CAD approach can effectively detect multiple independent attackers along a path. It provides High Packet Delivery Ratio with considerable overhead.

TABLE I. COMPARISON OF DIFFERENT TYPES OF DETECTION METHODS

DETECTION SCHEME	ATTACKS DETECTED	PROS	CONS
BSMR	Byzantine insider attacks	Software based solution , Can detect colluding attackers	Fails due to larger overhead
CHEMAS	Selective forwarding attacks	Larger detection rate	Fails due to larger overhead
Sprout	Greyhole and Blackhole Attack	Capable of detecting large number of colluding attackers	Chooses polluted routing path
MDT	Jamming, Greyhole and Sinkhole attacks	Reliable , high latency of reaching the base station	Collision occurs due to Same packet reaching the base station via different topologies
LEDs	Denial of Service attacks	Provides various security services	Suffers from larger overhead, maximum usage of network resources
UNMASK	Control and Data plane attacks	Light weight scheme also uses LSR , a secure routing protocol.	Not applicable for mobile networks
CAD	Standalone Greyhole Attack.	Capable of Detecting many attacks and High Packet Delivery Ratio.	Inefficient in case of colluding attackers

3 PROBLEM DESCRIPTION

When connected to internet, the mesh routers form backbone to provide service to mesh clients (infrastructure WMNs). These mesh routers are less mobile and serves as gateways in few cases. An outside attacker may compromise a mesh router within the network and gain access to sensitive data like public, private and group keys and instructs the router to act in a malicious manner. Most of the routing protocols designed for WMNs, e.g., Ad hoc On-Demand Distance Vector (AODV) and Hybrid Wireless Mesh Protocol (HWMP), assume that all nodes faithfully forward packets. The protocols used in mesh networks do not contain self-contained security measures for detecting attacker nodes. In some cases a single mesh router in the packet forwarding path may be compromised i.e., standalone attacker can be easily detected by the acknowledgment sent by the other loyal routers within the network. This paper deals with colluding attackers i.e., two or more routers within the network may be compromised by the outside attacker.

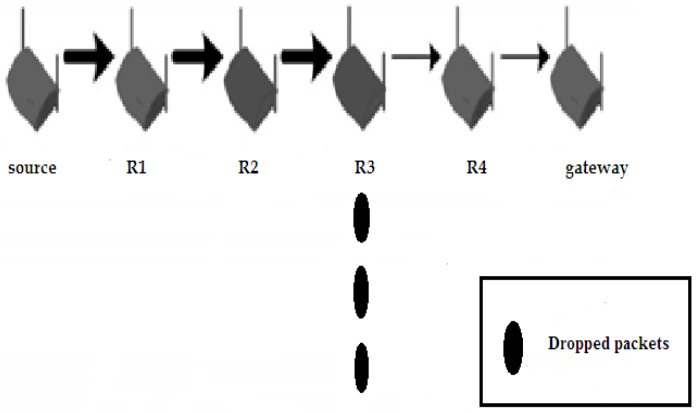

Fig 3.1. Selective forwarding attack

The Fig.1 shows the network model performing selective forwarding attack [21]. The network has a source that originates the information that must be passed to the destination via a gateway that connects the network to the internet. The router R_3 in the packet forwarding path acts as an inside attacker and cause packet loss. This router doesn't drop the entire dataflow packets instead drops sensitive data packets but forwards the control packets.

4 PROPOSED SYSTEM

4.1 Preview

The FADE (Forward Assessment based Detection) approach is used to detect the presence of colluding attackers in the WMNs. This approach has performance similar to that of CAD (Channel Aware Detection) with an extra advantage of detecting collaborative attackers in the network. FADE scheme adopts two strategies namely monitoring and multidimensional assessment.

FADE scheme apart from detecting colluding attackers it also detects multiple attacks like malicious accusation and counterfeit mark attack. FADE is a non-cryptographic scheme and runs in different underlying protocols. It must be assured that all the mesh nodes must be authenticated using the link layer security protocols thereby defending the network against external attackers from overhearing the message. Also the messages transmitted are further protected by key management techniques. Since link layer security is assured by the secured protocols and various encryption standards FADE technique is capable of detecting the attackers corrupting the network layer performance. Thus FADE scheme is used to differentiate the loyal nodes from the inside attackers in the network.

Monitoring: The behavior of both upstream and downstream nodes is assessed by two hop acknowledgement mechanism. The functioning of an intermediate node in the network is checked by the opinion of its both upstream and downstream nodes. The monitoring technique can detect standalone attackers in the network. The monitoring scheme uses acknowledgement from both upstream and downstream nodes to identify the loyalty of a particular node within the network.

Forwarding assessment based detection of attacks: By adopting multidimensional assessment, the normal behavior of a node can be determined by using the opinion of both upstream and downstream nodes. By combining the opinion of downstream assessment and end-to-end assessment, collaborative greyhole attack can be detected. CAD approach which uses only monitoring is an effective Way of detecting only standalone attackers in the network. When it comes to colluding attackers, CAD approach is not applicable, hence FADE uses an additional multidimensional assessment technique.

4.2 Assumptions

It is assumed that the mesh nodes have no energy constraint and all the mesh nodes are assumed to be static, forming a mesh backbone for infrastructure WMNs. The dynamic topology, decentralized and self-organizing nature of WMNs makes it prone to attacks. The following assumptions are considered in the proposed technique. The network is considered to be strongly connected. There occur a number of paths between the source and destination. The protocol uses the best path between the source to destination for the packet transmission. The mesh routers are highly authenticated and the secure encryption techniques are adopted. All the routers in the network have sufficient memory to store the packets received.

4.3 Forward Assessment based Detection

The FADE scheme works in three phases 1) Attack Information Collection, 2) Attack Detection, 3) Attack Reaction. It is presumed that the packet dropping is only due to poor channel quality, MAC Collisions and the presence of attackers within the network.

The proposed scheme uses optimum threshold levels to differentiate the packet loss due to attackers from other reasons. These thresholds are configured by estimation the normal losses due to MAC collisions and Poor channel quality. They also consider probability of false alarm rates in both conditions to avoid false threat detection.

1) *Attack Information Collection*: In FADE Scheme, the source node within the network generates challenge packets for collecting information about attacks. Every intermediate node maintains two counters, one for the number of data packets received and the other for two hop acknowledgement. The first counter value gets incremented for every data packet received which helps to identify normal behavior of that node. The second counter value gets incremented for every data packets forwarded to the downstream node which helps to identify the forwarding nature of its downstream node. Once the intermediate node receives the challenge packet adds its opinion about the downstream node. These challenge packets are generated by source nodes and are transmitted throughout the entire intermediate nodes present along the route. These challenge packets are highly secured by using ECDSA (Elliptical Curve Digital Signature Algorithm). ECDSA is a type of DSA using elliptical Curve cryptography. It uses curve parameters for key generation purpose. The Challenge messages are further encrypted using ADHASH to improve the efficiency of the key used for encryption.

2)*Attack Detection*: In attack detection phase more than a single attack is detected. This phase involves four cases depending on the end-to-end opinion and the opinion of the intermediate nodes

i. When opinion of both end-to-end nodes and downstream nodes are 0, this denotes the presence of no selective forwarding attacks in the network.
ii. When opinion of both end-to-end nodes and downstream nodes are1, this denotes the presence of standalone attackers in the network. Here in this attack a single attacker within the network drops packets. The CAD approach is capable of detecting standalone greyhole attacker within the network.
iii. When the opinion of downstream node is 0 and end-to-end opinion is 1, this case denotes the presence of collaborative greyhole attack. In this case, the attackers act in colluding manner i.e., one node in the network may act as an attacker and the other node may hide the packet drop done by the attacker node.
iv. When the opinion of downstream node is 1 and end-to-end opinion is 0. This case suggests two possible attacks. One is the malicious accusation attack by upstream node, and the other is the counterfeit mark attack by downstream node. For the malicious accusation attack, the upstream node intentionally accuses its downstream node regardless of its normal forwarding behaviors.

For counterfeit mark attack, the node drops few data packets and it itself changes the counter values in the packet received to provide positive evidences for showing itself as a loyal node. A feasible method to distinguish the two attacks is to check the link acknowledgements received.

3) *Attack Reaction*: when the challenge node generated by source node after traversing through all the intermediate nodes reaches the destination. The destination node generates a reply message for the challenge packet received from the source node. The source node performs attack reaction after the reply message received. There occurs three cases

i. When the source node receives a positive reply, it indicates the presence of no attack within the network.
ii. When the source node receives a negative reply, it indicates the presence of some attacks within the network.
iii. When the reply message does not reach the source node within the estimated time interval, thereby considering the presence of attack within the network.

5 SIMULATION RESULTS

The simulation is performed in network simulator ns2 (v2.33) with a network containing an average of 45 stationary nodes (numbered 0 to 44). ns2 use Tcl language for creating simulation scenario file (for example, sample.tcl). Network topology, transmission time, using protocols is defined in scenario file. The visualization tools are nam (network animator) fie and X graph. The nam file is a packet level animator well supported by ns2. The X graph provides the simulation results in the form of graph. The routing protocol used in DSR.

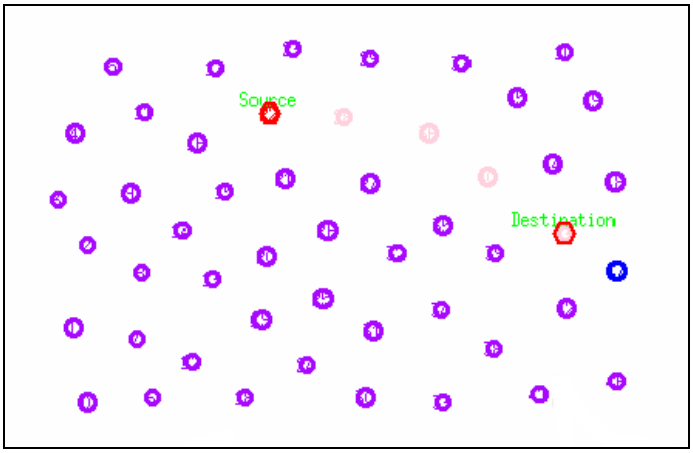

fig 5.1 Establishing Route Between Source To Destination

The fig 5.1shows the route establishment between source to destination occurs and normal data transmission takes place without the presence of attacker.

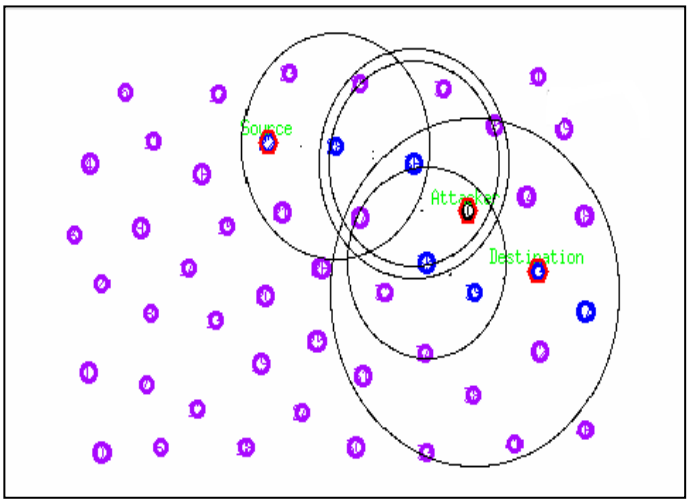

fig 5.2 Packet Transmission In The Presence Of Attacker

The fig 5.2 shows network with attacker in the path of data transmission. The attacker cause packet loss and FADE scheme running in the underlying protocol detects the presence of attacker in the network by the above discussed strategies.

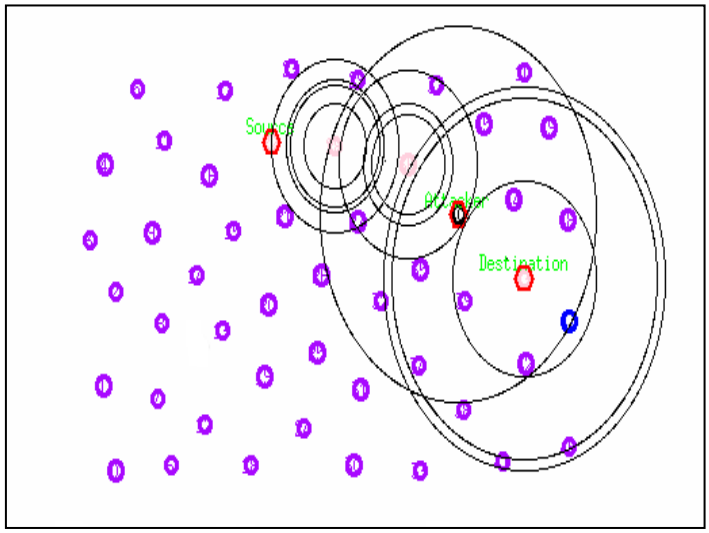

fig 5.3 Rerouting In A New Path After Detection Of Attacker

The fig 5.3 shows the rerouting of the path by eliminating the attacker from the network.

fig 5.4 Packet Delivery Ratio

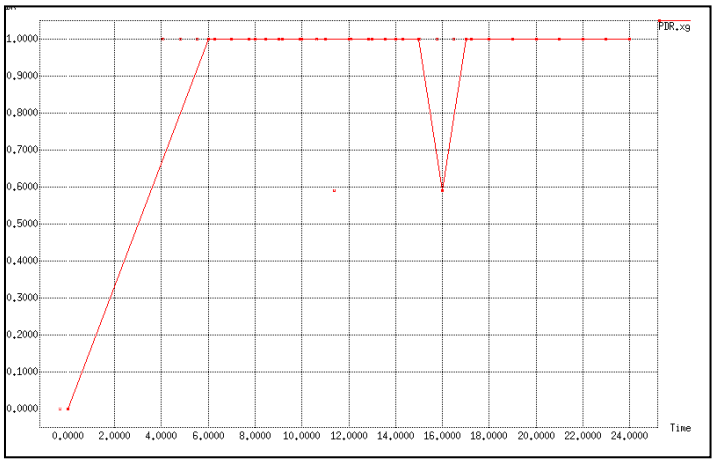

fig 5.4 Packet Delivery Ratio

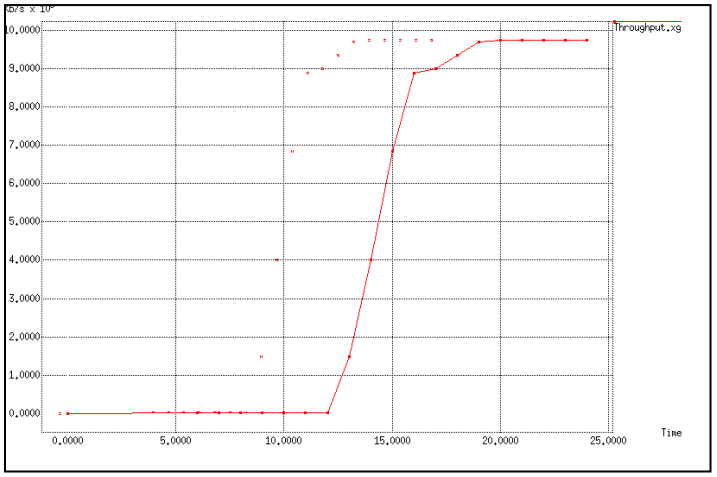

fig 5.5 Throughput

The FADE scheme provides high packet delivery ratio and throughput.

4 CONCLUSION AND FUTURE WORK

WMNs are used for military applications where secure routing of information is the major requirement. The FADE scheme uses both monitoring and multidimensional assessment techniques to detect the colluding attackers within the network. Apart from only detection of attacker in the routing path, this scheme also reroute the packets in a new path eliminating the attacker from the data forwarding path. This scheme is very effective in detecting the attacker within the network, hence a secure routing concept may be adopted in resolving and removing the attacker from the network.

ACKNOWLEDGMENT

I would like to thank authors, mentioned in the references which are citied below for their valuable research works which helped me to gain knowledge. And also I thank my guide for her precious guidance.

REFERENCES

[1] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures" Elsvier's Ad Hoc J., vol 1 no. 2-3 pp 293-315 Sept 2003.

[2] F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Commun. Mag.*, vol. 43, no. 9, pp. S23-S30, Sept. 2005.

[3] R. Curtmola and C. Nita-Rotaru, "BSMR: Byzantine-resilient secure multicast routing in multi-hop wireless networks," in *Proc. Sensor, Meshand Ad Hoc Communications and Networks*, June 2007.

[4] Gao Xiaopeng and Chen wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks" ,IFIP International Conference on Network and Parallel Computing Workshops 2007, pp 209-214, Sept 2007.

[5] B. Xiao, B. Yu, and C. Gao, "CHEMAS: identify suspect nodes in selective forwarding attacks," *J. Parallel and Distrib. Computing*, vol. 67, no. 11, pp. 1218-1230, Nov. 2007.

[6] J. Eriksson,M. Falaotsos, and S.V. Krishnamurthy, "Routing amid colluding Attackers," in Proc. 2007 ICNP, pp. 184-193

[7] H.N. Sun, C. M. CHEN and Y. C. H Asiao, " An efficient countermeasures to the selective forwarding attack in wireless sensor networks " in Proc. 2007 TENCON pp. 1-4.

[8] D. Manikantan Shila and T. Anjali, "Defending selective forwarding attacks in mesh networks," in *Proc. 2008 Electro/Information Technology Conference* , Ames, IA, May 2008.

[9] K. Ren, W. Lou, Y. Jhong : LEDs : providing location aware end-to-end data security in wireless networks" IEEE Trans. Comput. ,vol. 7,no. 5, pp 585-598, 2008.

[10] F. Oliviero and S. P. Romano, "A reputation-based metric for secure routing in wireless mesh networks," in Proc. 2008, GLOBECOM, pp. 1-5.

[11] D. M. Shila and T. Anjali, " A Game Theoretic Approach to gray hole attacks in wireless mesh networks", IEEE International Conference on Military communications 2008, pp. 1-7, Nov 2008

[12] W.Wang, B. Bhargava and M. Linderman, "Defending against collaborative packet drop attacks on manets" in DNCMS2009.

[13] M. Tiwari, K. V. Arya, R. Choudhary and K.S. Choudhary, "Designing intrusion to detect black hole and selective forwarding attacking in WSN based in local information" in Proc. 2009 ICCIT, pp. 824-828.

[14] S. Khan, K.-K. Loo, N. Mast, T. Naeem, " SRPM: Secure Routing protocol for IEEE 802.11 infrastructure based wireless mesh networks," J. Netw. Syst. Manage., vol. 18,no. 2,pp. 190-209, 2010.

[15] Khalil, S. Bagchi, C. N. Rotaru and n. B. Shroff, " Unmask: utilizing neighbour monitoring for attack mitigation in multihop wireless sensor networks" Ad Hoc Netw. Vol 8, no. 2, pp 148-164, 2010.

[16] Sahil Seth, Anil Gankotiya, "Denial of service attacks and detection methods in wireless mesh networks" ITC 2010, pp. 238-240.

[17] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating selective forwarding attacks with a channel-aware approach in WMN's," IEEE Trans. Wireless Commun.,vol. 9, no. 5, pp. 1661-1675,2011.

[18] V. V. V and V.M. A. Rajan, "Detection of colluding selective forwarding nodes in wireless mesh networks based on channel aware detection algorithm" MES J. Technol. Manage., pp. 62-66, 2011.

[19] Monika, "Denial of Service Attacks in Wireless mesh networks," IJCSIT Vol 3 (3), pp4516-4522, 2012.

[20] Yashpal Rohilla and Preeti Gulia, " A Comparative Study of Wireless Mesh and ad-hoc network : A CrossLayer design approach," IJCSE. Vol. 4,pp. 1181-1184, June 2012.

[21] Quiang Liu, Jianping Yin, Victor C. M.Leung, ZhipingCai, "FADE: Forwarding Assessment Based Detection of collaborative gray hole attacks in WMN's" IEEE Transactions on Wireless Communications, Vol. 12, no. 10, October 2013, pp. 5124-5137.