ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 9, November 2012

A defending of wormhole attack in wireless mesh network based on epigraph relay method and cooperative threading technique

Akshita Rana[1],Deepak shrivastava[2]

Research scholar, Research scholar[2]

Department of Electronic and Communication, Madhav Institute Of Technology and Science,Gwalior (474005)

Abstract—

The proper management of wireless mesh network is a challenging task due to the mobility of node and velocity of node. All devices work in open channel area due to this security is very challenging task. Because due to mobility and open channel area possibility of threats and attacks are very high. On the basis of related work we found data wormhole attack is a serious attack in the environments of wireless mesh network. Various methods and applications are used for the prevention of wormhole attack, but all these method and process are not up to mark. Now we get idea about wormhole attack and prevention of wormhole attack. Here any method or process does not work in the level of network for the prevention of wormhole attack. In this dissertation we proposed a new model for prevention and detection of wormhole attack in wireless mesh network. The proposed model based on epigraph relay method (ERM) and cooperative threading process.

Keywords: - WMN, Wormhole attack, ERM, threading

INTRODUCTION

Wireless mesh network is a network which is consisted of routers and clients organized in mesh topology manner and routers have rare mobility. Mesh routers work as gateway and clients are laptop, cell phone and other wireless devices. Mesh routers forward the packet at desired place with the help of other nodes [3,4]. It is a type of mobile ad-hoc network. Although wireless mesh networks are reliable but some redundancies are also offered by it. Wireless mesh network provides cost effective and dynamic connectivity and has more planned configuration where nodes automatically establishes and maintains the connectivity with other nodes in the network. Because of these properties wireless mesh networks are easy to maintain robust and reliable in service coverage [7,8]. Wireless mesh network can be used according to the need of communication as required in emergency situations, high speed mobile video applications on board public transport or real time racing car telemetry. Multicasting is a type of delivering messages from one node to set of nodes simultaneously in efficient manner [10]. In the multicasting process the message is transmitted only once (no retransmission) over the network and is duplicated only at the branch point. It reduces the bandwidth consumption in network which is possible in videoconferencing and distributed gaming like environment, where the same channel is accessed by many users. The protocols used in multicasting can be categorized in two types 1) Source Based Multicasting Protocols (ADMR, MAODV) and 2) Mesh Based Multicasting Protocols (ODMRP, CAMP)[12]. During transmission messages can be stolen and altered or services disruption is also possible in the network; which is called attack. There are many types of attack: 1) Active attack where intention is to alter the information and make the network overload, 2) Passive attack where intention is to steal the message and eavesdrop on the communication, 3) Impression attack which is also known as spoofing where attacker assumes the identity of another node in the network, so that receiving messages directed to the node it fakes, 4) Sinkhole attack where a compromised node tries to attract the data to itself from all neighboring nodes using loopholes in routing algorithms and 5) Wormholes attacks where a malicious node uses a path outside the network to route messages to another compromised node at some other location in the network.
Transmitter [16]. The rest of paper is organized as follows. In Section II, related work III proposed model. In section IV simulation and result analysis. Results followed by a conclusion in Section V

II.RELATED WORK

In this section we discuss related work in the field of malicious attack in adhoc and wireless mesh network. Patroklosg. Argyroudis and Donalo'Mahony entitled "secure routing for mobile ad hoc networks" a survey of secure ad hoc routing protocols for mobile wireless

networks is presented [1]. A mobile ad hoc network is a collection of nodes that is connected through a wireless medium forming rapidly changing topologies. The widely accepted existing routing protocols designed to accommodate the needs of such self-organized networks do not address possible threats aiming at the disruption of the protocol itself. The assumption of a trusted environment is not one that can be realistically expected; hence, several efforts have been made toward the design of a secure and robust routing protocol for ad hoc networks. Although the authors mention challenges such as quality of service support and location-aided and power-aware routing approaches, there is no mention of security considerations.Kejun Liu, Jing Deng, Pramod K. Varshney and Kashyap Balakrishnan entitled "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in mantes" 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect is proposed [2]. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. Analytical and simulation results are presented to evaluate the performance of the proposed scheme. An investigation is done by the author that the performance degradation caused by such selfish (misbehaving) nodes in manets. Extensive simulations of the 2ACK scheme have been performed to evaluate its performance. Zonghua Zhang, Farid Nait-Abdesselam, Pin-Han Ho and Xiaodong Lin entitled "RADAR: a Reputation-based Scheme for Detecting Anomalous Nodes in Wireless Mesh Networks" a novel anomaly detection scheme, called RADAR, to detect anomalous mesh nodes in wmns is proposed [3]. RADAR scheme provides features for evaluate each node's behavior by abstracting and examining appropriate observations using reputation and captures the node's behavior drifts in terms of reputation by exploring their temporal and spatial properties respectively. Soufine Djahel, Farid Na¨ıt-Abdesselam and Ashfaq Khokhar entitled "An Acknowledgment-Based Scheme to Defend against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol" a problem of cooperative black hole attack is proposed [4]. Cooperative black hole attack results in dramatic disruption of the network performance. An acknowledgment based scheme to detect malicious nodes and isolate them from the forwarding process is proposed by the author. Cooperative black whole attack targets a proactive routing protocol, such as OLSR. This scheme mitigates the loss of topology information due to the dropping of Topology Control messages by attackers. Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour,Yoshiaki Nemoto and Nei Kato entitled "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" a new anomaly-detection scheme based on a dynamic learning process that allows the training data to be updated at particular time intervals is proposed [5]. This dynamic learning process calculates the projection distances based on multidimensional statistics using weighted coefficients and a forgetting curve. Authors' proposed system demonstrates an effective performance in terms of high drs and low fprs against five simulated attacks, in addition to the scalability of the proposed scheme clarified by the simulation results obtained from two distinct network topologies of varying sizes. Zhengming Li, Chunxiao Chigan and Danniel Wong entitled "AWF-NA: A Complete Solution for Tampered Packet Detection in vanets" a novel scheme called Autonomous Watchdog Formation is proposed [6]. Autonomous Watchdog Formation is enabled by 2-hop Neighborhood Awareness (AWF-NA), to ensure nodes automatically functioning as watchdogs to monitor the behaviors of the relaying nodes. It aims to detect and react at each hop, and stop any tampered packet from further propagation in spite of dishonest watchdogs and relaying nodes. Soufiene Djahel, Farid Nait-abdesselam and Zonghua Zhang entitled "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" packet dropping attack or black whole problem is proposed [7]. In packet dropping attack is a node denies to corporate or forwards each other's packet to save its resources or disrupt the communication. This problem arises due to limited buffer space in the MAC or Network Layer or Request to send requests reach to maximum number or packet is corrupted due to collision or interference in the network. There are basically three defense techniques to protect the MANET's packet dropping first defense aims to forbid the malicious nodes from participating in packet forwarding function, a second defense line is launched, which seeks to stimulate the cooperation among the router nodes via an economic model and third to reveal the identity of the malicious node and excludes it from the network. Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen entitled "A Survey on Trust Management for Mobile Ad Hoc Networks" management schemes in mantes to provide trust network protocol are surveyed [8]. Trust is a degree of belief about behavior of a particular entity. Author suggests various design concepts to develop a MANET trust management system. Suggestions include that trust metric must have unique properties of trust, a trust management design must support cognitive functionality for each node to achieve adaptability to changing network conditions, a trust management system should be situation specific or situation aware, a trust management design must allow optimal settings to be identified under various network and environmental conditions so as to maximize the overall trust of the sys-tem for successful mission executions.

III PROPOSED MODEL

The proposed model based on epigraph relay method and cooperative threading process. Epigraph relay method well knows method for clock synchronization

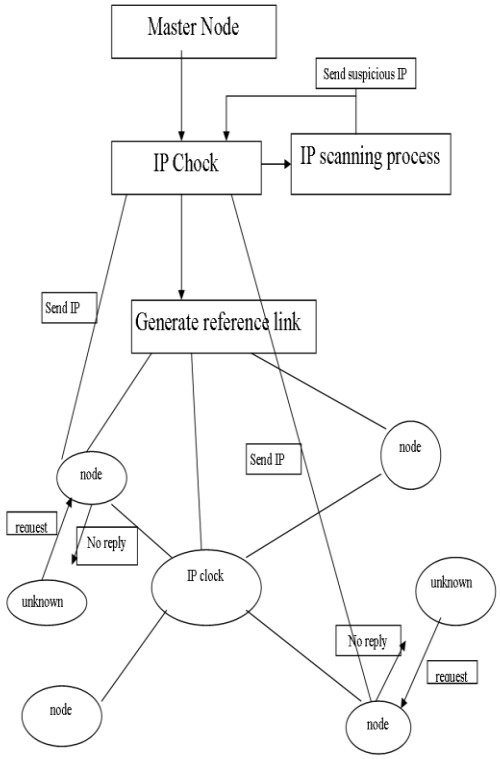
for receiver to receiver communication. Cooperative threading is a dynamic pointer, which generates a token value of parameter according to distance factor for every node in mesh network. Process of token generation is given below. For each token have offset value, clock and distance of relative reference node. The table is given below.

Sno.	Token	Clock	Distance
1	T1	3.4	1m
2	T2	4.5	2m
3	T3	3.5	1m
4	T4	7.9	3m

Offset value

Table 1: Token Generation

The receivers will compare their clocks to one another to calculate their phase offsets comparative. The timing is based on when the node receives the relative reference. The timing packet will be broadcasted to the receivers. The receivers will record when the packet was received according to their local clocks. Then, the receivers will exchange their timing information and be able to calculate the offset. If the measured time interval is within the range of offset value, the next hop node is considered as a legitimate node. In case the time interval exceeds the value of the offset value, the next hop node is set aside as malicious. Basically proposed work as a reference-packet filter, because in modern trend wormhole attack apply by the fake id packet and show the stable node of network. Attack share of information send by sender. So we design strong filter for unknown control request packet on the time of node mobility. In this process our methods generate a link for connecting a mobile node with their respective speed and all node connect our master node, basically master node is a nothing ,this is a control section of proposed and maintain all link from mobile node. Link of synchronization provided by clock. Clock maintains network ability for all nodes during communication. If unknown mobile node sends a request to any node, node not reply, node transfer that message to chock section chock scan their packet and find this is normal or abnormal and take action for blocking and generating a security alarm for all node. Our flow chart clear work view of model.



The compete block diagram of our proposed work

IV Simulation Results

For the effectiveness of our proposed model simulate in discrete network simulator ns-2, and used some standard parameter for performance analysis.

Parameter	Value
Simulation duration	100 sec
Simulation area	1000*1000
Number of mobile node	25
Traffic type	Cbr(udp)
Packet rate	4 packet/sec
Abnormal node	2
Host pause time	10sec

Table 1 shows that simulation parameter of our network

Performance Parameter

Throughput: It gives the fraction of the channel capacity used for useful transmission (Data packets correctly delivered to the destination) and is defined as the total number of packets received by the destination. It is in fact a measure of the effectiveness of a routing protocol [14]. Jitter: Jitter is the deviation in or displacement of some aspect of the pulses in a high-frequency digital signal. As the name suggests, jitter can be thought of as shaky pulses. The deviation can be in terms of amplitude, phase timing, or the width of the signal pulse. Another definition is that it is "the period frequency displacement of the signal from its ideal location"[7, 10].

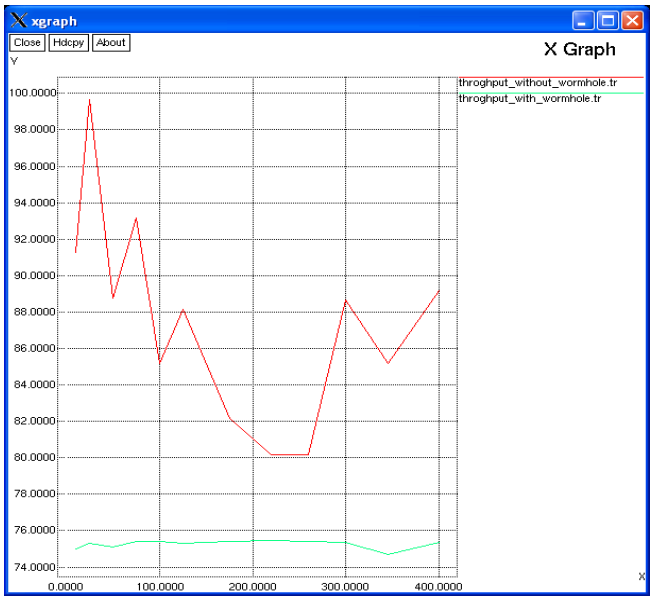


Figure 1 shows that comparative result analysis of throughput of wormhole attack and our defending technique of thread method.

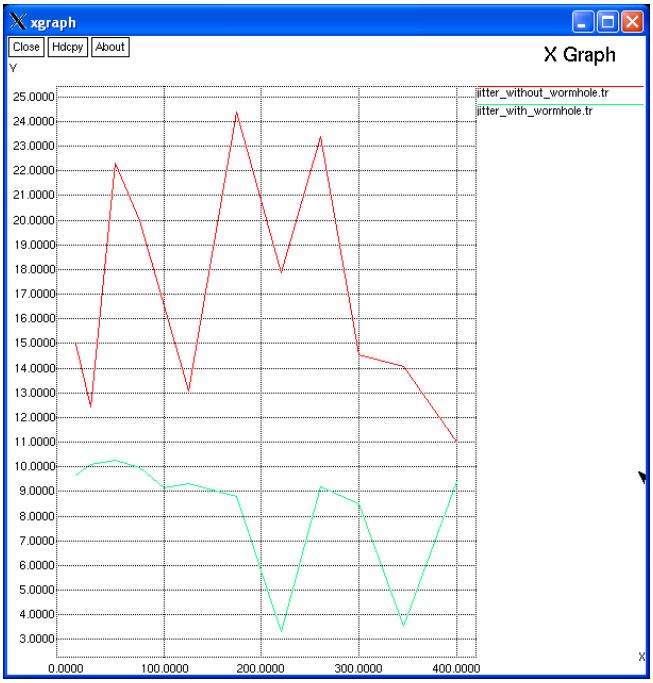


Figure 2 shows that comparative result analysis of jitter interval value of wormhole attack and our defending technique of thread method.

V CONCLUSION

In this paper we proposed a new technique for defending of wormhole attack in wireless mesh network. Our proposed method based on epigraph relay method and cooperative threading technique. Our evaluation result shows that better prediction of wormhole attack in wireless mess network. But due to thread generation it takes more time in comparison of another technique. In future we will minimize the calculation time of thread token generation and improve the efficiency of our proposed method.

REFERENCES

[1] Patroklosg. Argyroudis AND Donalo'Mahony "SECURE ROUTING FOR MOBILE AD HOC NETWORKS" in IEEE Communication, 2005.

[2] Kejun Liu, Jing Deng, Pramod K. Varshney and Kashyap Balakrishnan "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs" in IEEE Transaction, 2007.

[3] Zonghua Zhang, Farid Nait-Abdesselam, Pin-Han Ho and Xiaodong Lin "RADAR:aReputAtion-based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks" in IEEE Communications Society, 2008.

[4] Soufine Djahel, Farid Na¨ıt-Abdesselam and Ashfaq Khokhar "An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol" in IEEE Communications Society, 2008.

[5] Hidehisa Nakayama, Satoshi Kurosawa, Abbas Jamalipour,Yoshiaki Nemoto and Nei Kato "A Dynamic Anomaly Detection Scheme for AODV-Based Mobile Ad Hoc Networks" in IEEE Transactions On Vehicular Technology, 2009.

[6] Zhengming Li, Chunxiao Chigan and Danniel Wong "AWF-NA: A Complete Solution for Tampered Packet Detection in VANETs" in IEEE Communications Society, 2008.

[7] Soufiene Djahel, Farid Nait-abdesselam and Zonghua Zhang "Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges" in IEEE Communications Surveys, 2011.

[8] Jin-Hee Cho, Ananthram Swami and Ing-Ray Chen "A Survey on Trust Management for Mobile Ad Hoc Networks" in IEEE Communications Surveys, 2011.

[9] Jian-Ming Chang, Po-Chun Tsou, Han-Chieh Chao and Jiann-Liang Chen "CBDS: A Cooperative Bait Detection Scheme to Prevent Malicious Node for MANET Based on Hybrid Defense Architecture" in IEEE Transaction, 2011.

[10] Ian F. Akyildiz, Xudong Wang and Weilin Wang "Wireless mesh networks: a survey" in Science Direct, 2004.

[11] E.A.Mary Anita, V.Thulasi Bai, E.L.Kiran Raj and B.Prabhu "Defending against Worm Hole Attacks in Multicast Routing Protocols for Mobile Ad hoc Networks" in IEEE Transaction, 2011.

[12]Jin Xu "Multicast in Wireless Mesh Networks" in IEEE Transaction.

[13] Capkun S., Buttyan L. and Hubaux J. "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks" in ACM Workshop on Security of Ad Hoc and Sensor Networks (ACM SASN), 2003.

[14] Chiu H. S, Lui K. S. "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", In International Symposium on Wireless Pervasive Computing.

[15] Djenouri D., Khelladi L. and N. Badache "A Survey of Security Issues in Mobile Ad Hoc and Sensor Networks" in IEEE Communication Surveys & Tutorials, 2005.

[16] Hu Y-C., Perrig A. and Johnson D.B "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks" in proceedings of ACM Workshop on Wireless Security, 2003.

[17] Hu L., Evans D. "Using Directional Antennas to Prevent Wormhole Attacks" in Proceedings of the 11th Network and Distributed System Security Symposium, 2003.

[18] Khalil I., Bagchi S. and Shroff N.B. "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks" in International Conference on Dependable Systems and Networks, 2005.