World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(7): 73-77
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Pardeep Singh
Department of Computer Engineering, Guru Kashi University, Talwandi Sabo Bathinda, Punjab, India

Vijay Laxmi
Department of Computer Engineering, Guru Kashi University, Talwandi Sabo Bathinda, Punjab, India

Correspondence:
Pardeep Singh
Department of Computer Engineering, Guru Kashi University, Talwandi Sabo Bathinda, Punjab, India

Dynamic anomaly detection using cross layer security in MANET for Gray Hole Attack

Pardeep Singh,Vijay Laxmi

Abstract
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. Dynamic anomaly detection using cross layer security in MANET for GrayHole Attack is the working taken place in Link layer**.** It is the layer in which all the data will be send. Every request will be send in network layer. Relay nodes will forward the route requests in the network layer and receives the route replay in the data link layer. Any attacker node will work to destroy these layer. They will send the false route request and overload the node buffer by sending the false route request. 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: Gray Hole, AODV, Cross Layer.

Introduction
MANET is infrastructure less and self-configurable network where various users can communicate on temporary basis. It is collection of nodes that communicate with each other by the wireless links. Each node will work as source, destination and intermediate node i.e. work as switch.

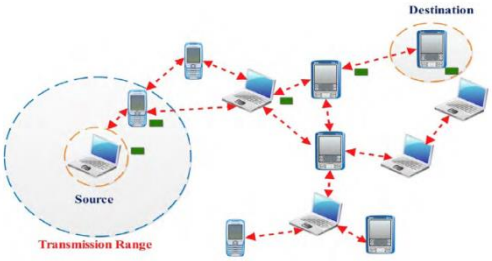


Fig. 1 [1]

Characteristics of MANET
- Dynamic topologies **:**In MANET nodes can join or leave network anytime so topology of network is completely unpredictable, route change are also frequent because if some node leave network it required to calculate another path for network topology.
- Self-organized: Mobile adhoc network provide high network agility they are self-organized and infrastructure less and quick deploy network, each node (device) in network act as relay agent and router perform packet forwarding and provide different network applications and services.
- Scalability: MANET provide great flexibility for users, due to wireless transmission medium it is very effective to cover remote sites and geographical distance areas.
- Multihop : MANET network node can communication only if there are in common radio cover range in MANET there are number of device present.

- Between sender and receiver and node are moving continuously message are forwarded from relay agent in network.
- Device heterogeneity: MANET consist devices such as PDA, Smart Phones. Laptops, thin client wearable devices can connect via wireless and create adhoc network.
- Cooperating: MANET are required coordination between node form packet forwarding to application and service delivery.in MANET each node act as client and server, node act as master or slave and each node have equal priority and service availability.

Applicatios of MANET

- Tactical networks: In military and battle field operations required adhoc network for communication with solders, vehicle, headquarter or check post and base camp.
- Emergency services**:** Establish network for Search and rescue operations in Disaster recovery.
- Transport and avian industry**:** vehicle are communicated with advance sensors in drives self-drive cars and Airplane and fighter jet communicated via adhoc network to detect and avoid collisions.
- Entertainment: Adhoc network used in playing multi-user game via wireless point to point network and outdoor access points.
- Sensor networks: Remote area monitoring, Field sensing and data gathering required a quick deployable network and Coverage extension of network.
- SOHO environment: In small office home office environment application like file sharing, data transfer, connecting printers, internet access.

Limitations of MANET

- Energy constraint: limited Energy in mobile devices they are power by batteries which have limited capacity small size of battery and heavy consumption make it more important constraint to think before we make any changes in existing solution. It is high priority requirement to make energy consumption as low as possible to increase node as well network life.
- Decentralized: MANET there is no central authority to monitor and coordinating network, so it is difficult to detect and prevent fault and issue in network.
- Routing overhead: Adhoc network node perform packet routing and routing lookup, due to dynamic nature of network node are moving so there is path breaks and frequent route lookup
- Limited Resources: Adhoc network used shared wireless medium there is limited bandwidth available for users in network.
- Environment impact: Wireless communication affect by following issues such as noise, frequency interference, signal attenuation, line-of-sight issue, radio signal path loss, multipath fading, diffraction and diffraction of radio wave.
- Security: Wireless nature of communication links make this network more susceptible and vulnerable for security threats like eavesdropping and traffic analysis. Limited resources make it an opportunity for attacker to target and degrade the expected performance. For example, DDOS attack or flooding attacks are used to increase bandwidth and battery consumption. It leads to degrade node life and delay in packet delivery.

Security in MANET

- Security: The aims of Ad hoc networks and mainly MANET have in recent years not only seen general use in commercial and domestic application areas but have also become the focus of intensive research. Applications of MANET's collection from simple wireless home and office networking to sensor networks and similarly constrained deliberate network environments. Security aspects play an important role in almost all of these application situations given in the wireless network.
- Protecting Mobile ad hoc networks: In the ad hoc networks, nodes do not start out aware with the topology of their networks instead, they have to discover it. The basic idea is that a new node may declare its presence and should listen for messages broadcast by its neighbours. Each node learns about neighboring node and how to reach them.
- Reactive approach: This type of protocols keeps new lists of destinations and their routes by periodically distributing routing tables in the network.
- Proactive approach: In proactive routing protocols the method is different than the reactive routing protocols. In this type of protocols essentially routes are depends upon the traffic control which is continuous. All routing information preserved at any time of the network because we know that network is dynamic which changes its size by making its size increasing or decreasing.

Related Work

G. Usha et al. (2016): Mobile ad hoc networks (MANETs) are one of the emerging technologies of wireless communication, in which each node in the MANET acts as a router. In an ad hoc network, any node can communicate with any other node in the network. However, this infrastructure of mobile nodes makes this system more vulnerable to various types of attacks. A black hole attack is one such attack in which the packet is dropped maliciously. In this paper, we propose a security solution known as the honeypot-based dynamic anomaly detection using cross-layer security (HBDADCS). The proposed technique detects and isolates black hole attacks from the ad hoc network. In this work, various novel algorithms are used which involve honeypot methodology. These technologies are proposed in order to detect and isolate black hole attacks from the network. Simulation-based results prove that the proposed technique has better packet delivery and end to end to delay with a decreased network load solely due to control packets compared to the other existing techniques.

Theofilos Chrysikos et al(2016): Wireless Information-Theoretic Security (WITS) has been suggested as a robust security scheme, especially for infrastructure-less networks. Based on the physical layer, WITS considers quasi-static Rayleigh fading instead of the classic Gaussian wiretap scenario. In this paper, the key parameters of WITS are investigated by implementing an 802.11n ad-hoc network in an outdoor obstacle-dense topology. Measurements performed throughout the topology allow for a realistic evaluation of a scenario with multiple moving

eavesdroppers. Low speed user movement has been considered, so that Doppler spread can be discarded. A set of discrete field test trials have been conducted, based on simulation of human mobility throughout an obstacle-constrained environment.

Sajal Sarkar et al(2016): In this paper they propose a game theoretic framework for stochastic multipath routing in mobile ad hoc networks (MANETs). In a MANET, intelligent and adaptive attackers may try to hijack, jam or intercept data packets traveling from source to destination. In this proposed game, at each stage the source node keeps track of the available multiple paths, the residual bandwidth of the paths and the strategy of the attackers from the information gathered during the previous stage. Based on these observations, the source node selects a path for data communication and switching strategy among the multiple established paths between the source node and the destination node.

N.Venkatadri et al (2016): Ad Hoc wireless network is a type of wireless network, in which there is no any fixed infrastructure. Devices in Ad Hoc network can move around the network within a given range. Currently most of the transactions are performed through the computer networks so they are more susceptible to many physical security threats. One of the major DOS Attacks that degrade the performance of the whole MANET is Black Hole attack. In the presence of black hole attack, nasty nodes are not forward the packets rather they drop packets.

In this work, black hole attack is detected and eliminated through implementing Digital Signature with Twofish Algorithm. We modified on-demand routing protocol Temporally Ordered Routing Algorithm (TORA) and named it as STORA. Our proposed STORA performs well under normal conditions and under black hole attack than original TORA.

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.

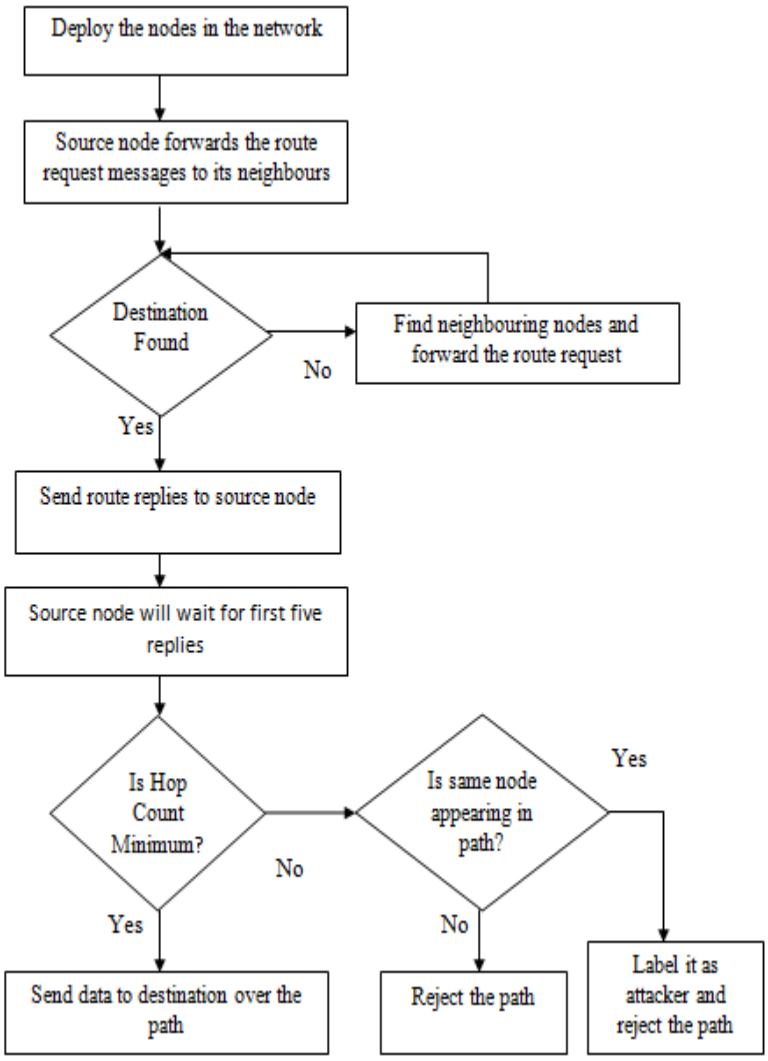
Step4: Send false destination request source nodes to the neighbors which are in the intermediate node list. If the reply then node will be considered malicious. else it will be declared legitimate.

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.

Flowchart



Results and Discussions

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.

Performance Parameters

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

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.

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.

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

MANET structure

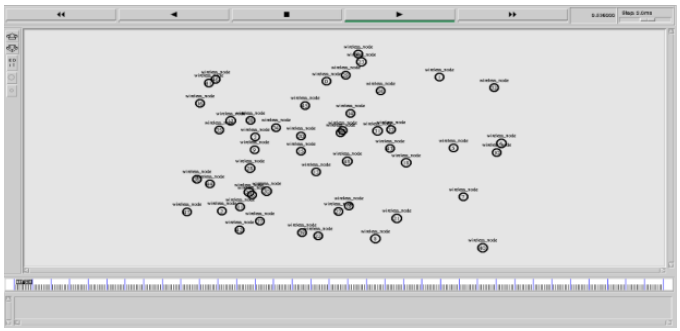


Fig. 2

This snapshot shows the MANET with wireless nodes. These nodes are randomly placed in specific area. All the nodes are moving randomly from one position to the other position. While moving they communicates to each other. The network builded using NS2 platform. These nodes moves in the range of 800,550 working range.

Grayhole Detection

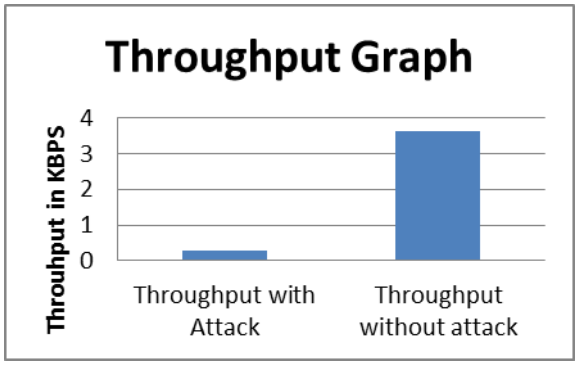
Fig. 3

This Figure shows the MANET with Grayhole attack. Our objective is to detect this gray hole attack using cross layer security. So that no attacker node can destroy the network. This type of attack detection is done using data link layer and transport layer.

Communicating Node and Gray hole

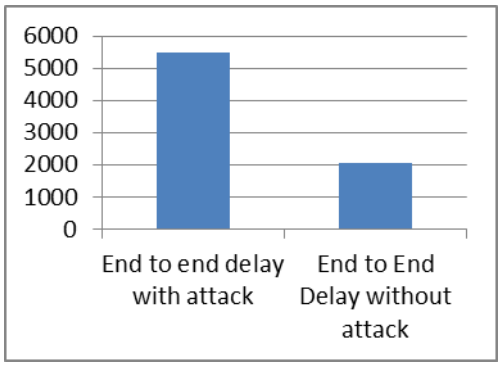
Fig. 4

Throughput Graph for Network with and Without Attack



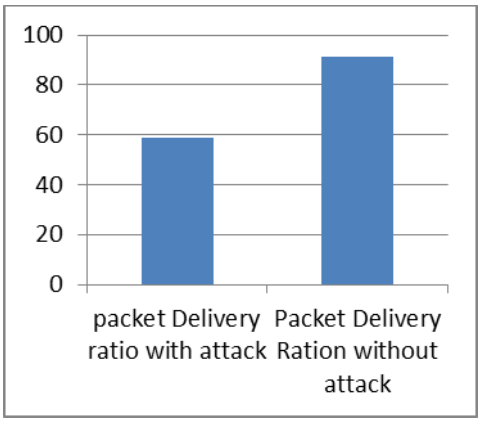
Graph 1.1

End to end Delay Graph for Network with and Without Attack



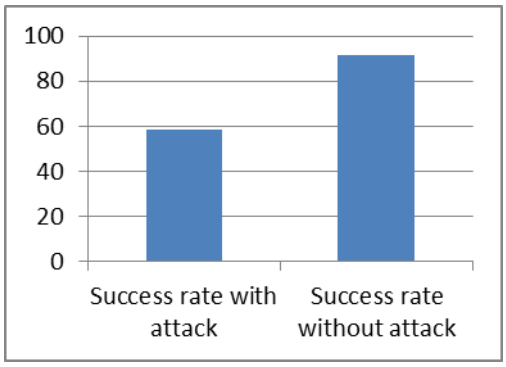
Graph 1.2

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

Percentage Improvement

Particular	Percentage
Throughput	92%
End to End Delay	66%
Packet Delivery ratio	35.88%
Success Rate	35.88%

Table 1.6

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 SAODV. As secured AODV. 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. G. Usha a, M. Rajesh Babu b, S. Saravana Kumar," Dynamic anomaly detection using cross layer security in MANET", Computers and Electrical Engineering (2016) 1–11.
2. Theofilos Chrysikos a,Konstantinos Birkos a, Tasos Dagiuklas b, Stavros Kotsopoulos," Wireless Information-Theoretic Security: Theoretical analysis & experimental measurements with multiple eavesdroppers in an outdoor obstacle-dense MANET", 18 November 2015
3. Sajal Sarkar a,Raja Datta," A game theoretic framework for stochastic multipath routing in self-organized MANETs", 16 February 2016.
4. N.Venkatadri, Reham Abdellatif Abouuhogail and Ahmed Yahya, "Secure TORA: Removal of Black Hole Attack using Twofish Algorithm", International Journal of Software Engineering and its Applications, 2016.
5. Pham Thi Ngoc Diep, Monika Sachdeva, "Detecting Colluding Blackhole and Greyhole ttack in Delay Tolerant Networks", ICRTEDC-2015, Vol. 1, Special Issue. 2.
6. Jaydip Sen," Detection of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", Bengal Intelligent Park, Salt Lake Electronic Complex, Kolkata, INDIA,2014
7. Bansi S. Kantariya1, Dr. Narendra M. Shekokar2," Detection and Mitigation of Greyhole Attack in Wireless Sensors Network Using Trust Mechanism", (2013)
8. Pham Thi Ngoc Diep," Detecting Colluding Blackhole and Greyhole Attack in Delay Tolerant Networks",2015.
9. Yanzhi Ren," Detecting Wormhole Attacks in Delay Tolerant Networks",2015
10. Harsh Pratap Singh," Cooperative Blackhole/ Grayhole Attack Detection and Prevention in Mobile Ad hoc Network: A Review", Volume 64– No.3, February 2013
11. Kanu Geete," A Survey on Grey Hole Attack in Wireless mesh Networks", Volume 95– No.23, June 2014
12. Akinlemi Olushola O, K. Suresh Babu, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007.
13. V. V. S. S. S. Balram, "A New Approach for Defending Against Vampire Attack in Wireless Sensor Networks," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 6, no. 1, pp. 501–505, 2016.