Enhanced Intrusion Detection Against Blackhole and Flooding Attack for Routing Protocol in MANET

Kunjan Shrivastava[1], L. K. Vishwamitra[2]
[1]*Department of Computer Science & Engineering, PCST, Bhopal, India*
[2]*Professor, Department of Computer Science & Engineering, PCST, Bhopal, India*

Abstract*— Networks are used in various fields. Network's popularity has motivated the development of mobile Ad-Hoc networks (MANETs). A mobile Ad-Hoc network is a kind of decentralized wireless system which creates a fast changing network. The inherent characteristics of MANET such as wireless medium, highly dynamic topology, distributed cooperation, resource constrained capability, and limited physical security poses number of nontrivial security challenges to the network. Hence, enforcement of security through secure routing protocol becomes an extremely critical task Mobile Ad-Hoc network has various kinds of security concern problems, which are caused by their nature of collaborative and open systems and by limited availability of assets. There are various Routing protocols in Mobile Ad-Hoc network but the Ad-Hoc on demand distance vector (AODV) is most popular widely used as it has many attributes. In this paper, we propose a solution to the black hole attack in one of the most prominent routing algorithm, Ad-Hoc on demand distance vector (AODV) routing, for the MANETs. The proposed method uses promiscuous mode to detect malicious node (black hole) and propagates the information of malicious node to all the other nodes in the network. The simulation results show the efficacy of the proposed method as throughput of the network does not deteriorate in presence of the back holes.

***Keywords* - Component; formatting; style; styling.**

I. INTRODUCTION

We can inspect the multilevel data packets even with compressed data. MANET Network is prone to highly vulnerable attacks due to its dynamic nature of Network infrastructure, among these Routing attacks received considerable attention since entire MANET structure will collapse on routing failures or router snooping. Existing methods will result in Node isolation which leads to unexpected network partition which may backfire rather than protecting. The studies on node capture attacks have all focused on the ability of an adversary to compromise the security of single-hop wireless links. However, messages in a wireless network traverse multiple links and paths between a source and destination node, and a message may be compromised by traversing a single insecure link.

The overall security of routed messages is thus dependent on the routing protocol implemented in the wireless network, as well as the physical network topology and the relative positions of the source and destination nodes in the network. Moreover, the fact that a message is transmitted over numerous links between a source and destination node implies that the overall confidentiality and integrity of the routed message may only be as secure as the least secure link, implying that vulnerabilities arise due to the topology of secure links in the wireless network. Hence, the impact of a node capture attack is a function of both the cryptographic protocol which provides link security and the routing protocol which determines the set of links traversed by a given message. Mobile Ad hoc Network (MANET) are a class of wireless communication networks without a fixed infrastructure.

The MANET concept basically evolved to tackle disaster situation like tsunami, earthquake, terrorist activities, battlefields, landslides, etc. Later, the concept has been extended to include applications such as online education, gaming, business, etc. Several applications in MANETs need group communication to manage the situations. The MANET nodes do not provide reliable services and QoS (Quality of Service) guarantees as compared to other wireless networks such as WiFi, WiMAX, GSM and CDMA. The main sources of unreliability in MANETs are due to limited battery capacity, limited memory and processing power, varying channel conditions, less stability under unpredictable and high mobility of nodes. The QoS parameters to be guaranteed for multimedia group communication are bandwidth, delay, packet loss, jitters and bandwidth-delay product Ad hoc networks consist of hosts interconnected by routers without a fixed infrastructure and can be arranged dynamically. Considerable work has been done in the development of routing protocols in different types of ad hoc networks like MANETs, WMNs, WSNs, and VANETS etc [1]. In recent years, the interest in ad hoc networks has grown due to the availability of wireless communication devices that work in the ISM bands. While designing an ad hoc network in particular we are concerned with the capabilities and limitations that the physical layer imposes on the network performance. Since in wireless networks the radio communication links are unreliable so it is desirable to come up with an integrated design comprising of physical, MAC and network layers[2]. The main vision of MANET is to support robust and efficient operation in wireless networks by incorporating routing functionalities at each mobile node. For such designing aspects of ad hoc networks Routing based approach, Information-theoretic approach, Dynamic control approach or Game- theoretic approach has been implemented [3].

In MANET to support mobile computing a mobile host must be able to communicate with other mobile hosts which may not lie within it' s radio transmission range. Hence routing protocols will need to perform four important functions as determination of network topology, maintaining network connectivity, transmission scheduling and channel assignment, and packet routing. Routing protocols in MANETs were developed based on the design goals of minimal control overhead, minimal processing overhead, multi hop routing capability, dynamic topology maintenance and loop prevention [1].

II. SECURITY CONSIDERATIONS

We aim at achieving a security enhanced MANET protocol that fulfils the following main objectives. The objectives mitigate threats that are relevant in practice. The proposed concept is described in subsequent chapters.

Protection of communication channels:

In MANETs, communication between wireless devices is realized via an open broadcast medium. Compatible devices, in the range of a sending device are capable of receiving all contents of the transmission. Furthermore, they are capable of sending similar or equal contents on the medium. So far, security was not in the focus of the design of these networks. The proposed concept implements mechanisms for the protection of communication channels. It achieves confidentiality of all transmitted data on a hop-by-hop (direct link) basis and it protects from eavesdropping. Authentication and integrity assessment of a remote device precedes any data transmission. Protected communication channels are established in the field. All devices within transmission range exchange shared secrets for the protection of transmissions. The key exchange mechanism also uses the TPM whereby hardware protection against man-in the-middle -type threats is achieved.

Protection of privacy:

The provided solution protects the privacy of users of a device against peers. Unintended traceability, recognition and assignment of single device, and thereby its user, is confined to the link-layer. Pseudonymous TPM keys, the secured key exchange and transmission mechanisms support the protection of privacy. Solutions on higher and lower communication layers, as well as revealing device characteristics, are not in focus of this work. Cross-layer security is e.g. discussed in [4].

Protection of routing tables:

Routing tables have to be protected from malicious manipulation in order to counter a variety of threats. Unsecured MANETs suffer from outsider and insider attacks, aiming to inject wrong routing information (e.g. black hole, loops). The dissemination of maliciously manipulated routing information must be prevented. For our solution it is assumed that devices with a correct software state do not manipulate routing information maliciously. Thus, attacks either come from outsider devices or from manipulated software on known devices. The TPM and its integrity measurement mechanisms allow devices to recognize manipulations of neighbouring devices. Routing messages of manipulated devices are dropped and not forwarded in the network.

Protection of cryptographic keys:

Capturing of devices by an adversary is a serious concern for mobile equipment. Especially, pre-shared keys need to be protected even if devices are stolen. The provided solution does not require any pre-shared and MANET-wide symmetric keys which are expected to increase the vulnerability of the whole network. Instead it relies on asymmetric keys stored in the TPM. Identity keys and storage keys cannot be compromised by software means. Physical manipulations to TPMs are possible but difficult, expensive and time consuming. All other cryptographic keys utilized in the communication between devices are freshly created, bound to a well known system state and of short temporal validity.

Trust in MANET:

Trust is a very acute feature that be influenced by on indeterminate situations and is used for judgment building on collaborating with strange members. It comprises creation and updation of trust. In overall, trust administration and status administration are always used but it is not always the fact. There always lies a variance between the trust and reputation. Golbeck [5] explains nearly three main assets of trust in order to social network. Trust could not be totally transitive in terms of mathematical. For example, if X trusts Y, and Y trusts Z, it does not guarantee that X trusts Z.

III. ROUTING ATTACKS IN MANET

There are various means and ways to attacks in MANET by malicious node(s), for example, sending false messages numerous times, false routing data, and promoting false links to disorder routing actions. Various routing attacks against MANET [5] protocols are deliberated in brief. Here some of the critical and vital routing attacks are taken in consideration.

3.1 Flooding attack (DoS)

Attacker is meant for exhausting the mobile Ad-Hoc network's all resources, for example bandwidth and other resources of a node, for example computational efforts and battery energy or to interrupt the routing main operations to reason undecorated degradation in performance of network. Such as, AODV [6] protocol, any malicious node could spread huge number of RREQs in a very short span of time to a target node which does not exist actually in the network. For this situation, no node would reply to these RREQs, and finally this request, RREQs, would flood the whole ad hoc network. In the result form, all of the nodes of Ad-Hoc network get overwhelm with battery power and network bandwidth of network would be spent and could prime to denial-of service.

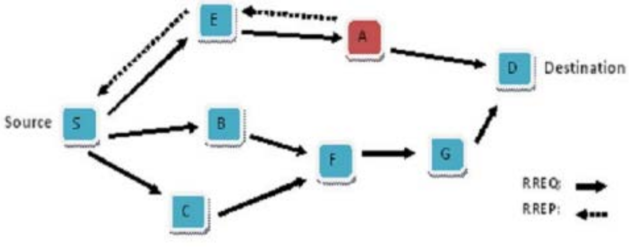


Fig 1: Blackhole Attack in AODV

3.2 Blackhole attack

A black hole is created with the opponent at the main centre. The opponent traps the traffic of the network close to a compromised in this type of attack. Basically the attacker offers an attractive path to the neighbouring nodes. This attack can also be paired with other attacks like packets dropping, denial of service, replay of knowledge, selective forwarding [7].

3.3 Link spoofing attack

This is an attack where a malicious node broadcast false links with all those nodes which are not direct neighbours of the node to interrupt routing operations. Such as, in the OLSR, an attacker could spread a false link with a all those nodes which have target's two-hop neighbours. And undoubtedly, this serious reasons the group of target nodes to choice the malicious node, which is to be its own MPR [7].

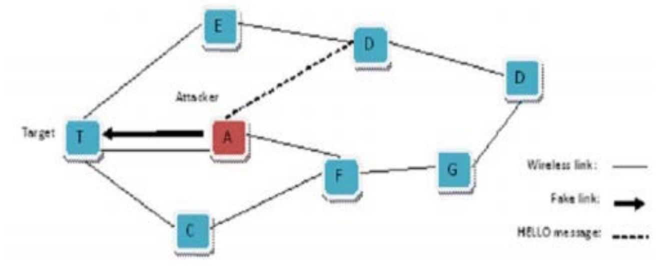


Fig 2: Link Spoofing Attack

3.4 Wormhole attack

Here the opponent connects two distant parts of the network and convey messages received in different part of the network to the other. A lower latency link is used to pass the messages in this type of network [7].

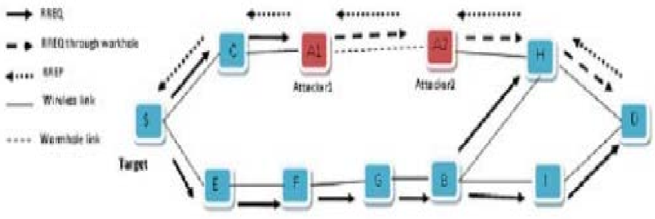


Fig 3: Wormwhole Attack on reactive routing.

IV. RELATED WORK

AODV routing protocol performs both unicast and multicast routing. It maintains the route as long as they are needed by the source node. It uses the sequence number field to avoid the looping and to ensure the freshness of the route. As wireless network are prone to path breakage due to the mobility of the nodes, fading environment etc., so it is beneficial to provide some stable routes which can improves the performance of AODV protocol. Many researchers have proposed changes in the AODV protocol for increasing the efficiency, stability and security [8] [9] [10] of the MANETs. The main problems that should be considered are energy efficiency and security in Ad-Hoc networks.

The resources present in MANET are limited, e.g., battery power MANET is very important resource as it has limited life and are not easily rechargeable. So we have to reduce the energy consumption in MANET by using an efficient routing algorithm for data transmission. Considering the above problems Gomez et al. proposed the PARO protocol which evaluated the distance between two nodes and after the distance calculation determine the transmission power needed to reduce power consumption. In PARO protocol it is assumed that each node can directly communicate with the other entire node in the network (a one-hop network). A sending node uses the maximum power to transmit the first packet to the destination node and receives the ACK packet from destination. Then it determines the distance from itself to destination node and computes the minimum power needed for data transmission. Because the network is fully connected in PARO, broadcasting messages to the source and the destination node result in extra power consumption.

Yang et al. have proposed a PAMP (Power aware multipath routing protocol) where routes are created by calculating the remaining power of nodes and recorded in RREQ packets. When destination node receives this RREQ packet it calculates the amount of power needed for data transmission and compares the both. If remaining power is less than the required power then destination node waits for the next RREQ consequently very long delay occurs in the route creation process. Wang et al. have proposed a power efficient routing and maintenance protocol in MANET which removes some drawbacks of PAMP protocol. This protocol mainly considers the transmission bandwidth between two nodes and creates the routes on the basis of the power available for the data transmission in those routes. Vadival et al. have proposed energy efficient with secured reliable routing protocol (EESRRP) for MANET. This protocol creates the routes on the basis of some threshold value of the power and packet drop ratio using AODV protocol. A new power aware multicast routing protocol for MANET which similar to the PAMP protocol but has less overheads is proposed by Varaprasad et al. If path breakage occurs in the MANET then lot of energy wasted in the creation of the new routes, due to flooding of RREQ packets. Pan et al. have proposed a local repair mechanism for on-demand routing in MANET.

This protocol repairs the route locally whenever route breakage occurs, without notifying the RERR message to the source node and reduces the overheads of route maintenance. But they did not consider the security and the battery power of the nodes. Security in MANET is another big issue in current days. The proper security mechanism for detecting the possible attacks in AODV routing protocol needs to be incorporated for the security. Much type of attacks are possible in MANET and the most frequent one is packet dropping attack. John and Vivekanandan have proposed a framework for secure routing in Mobile and Ad-Hoc network. This protocol focus on cooperation in packet forwarding. A context-free protocol there is no need to know whether nodes are selfish are not, so this protocol does not need to track node’s behavior to build a context consequently avoiding all the troubles caused by context maintenance. Such a context-free solution is very different from traditional context-based ones and must be designed in a totally new way. But in this protocol security mainly depends on the cooperation of the nodes. A secure energy efficient routing protocol for wireless Ad-Hoc networks has been proposed by Mahimkar et al. which selects the paths along nodes with a higher reputation number and higher residual battery capacity.

In Mobile and Ad-Hoc network the power with the node is a scarce resource, which cannot be replaced. Also the very applications of MANET for real life scenario makes it prone to attack by the external/internal agencies. Many methods have been proposed to look in to those problems but a lot of overhead is associated with them. Therefore, in this work an energy shaving routing scheme using dynamic route shortening and local route repair mechanism id developed. A security mechanism is also designed by using the trust value of the node to locate the reliable communication path which detects the malicious node in the network.

V. PROPOSED WORK

It is necessary that no node could identify packet format during packet delivering process. Our proposed approach does exactly the same We propose a method which uses promiscuous mode of the node. This mode allows a node to intercept and read each network packet that arrives in its entirety, in other words, promiscuous mode means that if a node A within the range of node B, it can overhear communication to and from B even if those communication do not directly involve A.

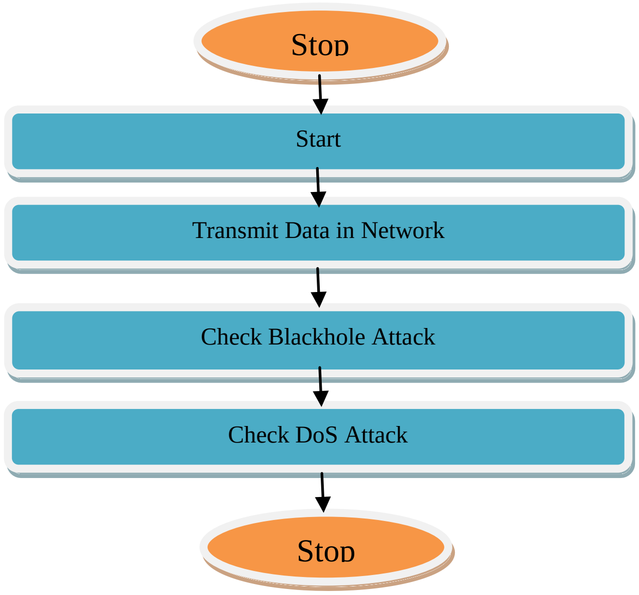


Fig 4: Algorithm of Proposed Work

VI. SIMULATION AND RESULT ANALYSIS

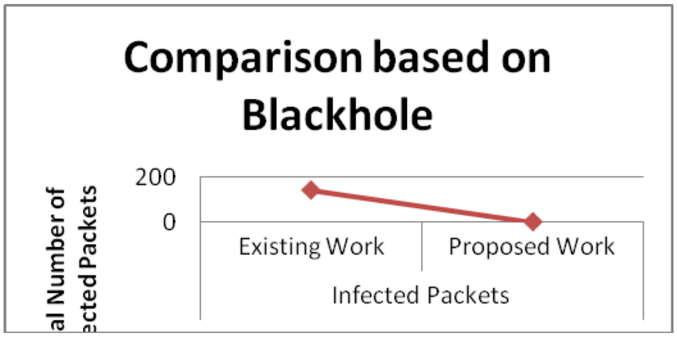
The performance of proposed algorithms is implemented on network simulator (NS-2) and the results are compared with original AODV to check the performance. So by the result comparison we can say the now there are less blackhole effects in the network and now AODV performs better than the original AODV. To reduce the packet dropping attack in the network the security mechanism is implemented a new Format Packet in the network and hence improving the performance of the network by, reducing infected number of packets in attack environment in the network. The simulation parameters used to implement the proposed algorithms have been tabulated in Table 1.

TABLE 1: SIMULATION PARAMETERS USED IN SIMULATION

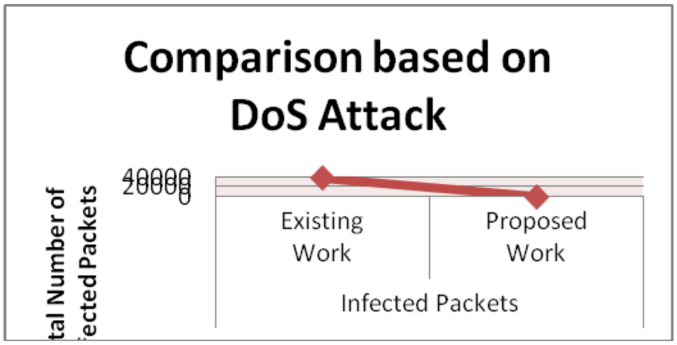
Simulation Time	360 seconds
Protocol	AODV and AFP(Developed)
Area:	800 x800
Traffic	APF1/APF2
Channel	Wireless
Operation mode	802.11
Mobility	Random waypoint
Antenna	Omni directional
IFQ	100
Nodes	50
IFQLEN	1000

The following parameters have been used for evaluation of the performance of proposed algorithms:

Number of infected Nodes: The total number of infected nodes in the Adhoc network. First of all we presents the results of security implementation part. The results are computed by tracing the output files generated by NS-2 simulator during simulation for all the proposed approaches. The performance of proposed algorithms are evaluated on the network with 50 nodes.



Graph 1: It shows the number of Blackhole infected packets after implementing Existing work and proposed work



Graph 2: It shows the number of DoS infected packets after implementing Existing work and proposed work.

Graphs 1, 2 and explicitly shows that the performance of the our proposed corporative Intrusion Detection System work over existing work.

VII. CONCLUSION

MANET is an emerging area as it has great potential in various diverse areas, e.g., military, disaster management, intelligent transportation system, monitoring, public safety. In this paper, we discuss blackhole and DoS attacks which is a severe security risk in routing. We have proposed a simple, efficient and effective method with maximizing Packet Delivery Ration to overcome the problem of the black hole and DoS attack problem. The proposed method uses promiscuous mode of a node to overhear the neighbor's communication. It does not require any database, extra memory and more processing power. The simulation results show effectiveness of the proposed method over existing method on various parameters.

REFERENCES

[1] Kannhavong B, Nakayama H, Nemoto Y, Kato N, and Jamalipour A,
"A Survey of Routing Attacks in Mobile Ad Hoc Networks,"IEEE
Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007.

[2] Marti S, Giuli T, Lai K, and Baker M,"Mitigating Routing Misbehavior
in Mobile Ad Hoc Networks,"Proc.ACM MobiCom,pp. 255-265,2000.

[3] Hu Y, Johnson D, and Perrig A, "SEAD: Secure Efficient Distance
Vector Routing for Mobile Wireless Ad Hoc Networks," Ad Hoc
Networks, vol. 1, no. 1, pp. 175-192, 2003.

[4] D. Kidston, L. Li, H. Tang, and P. Mason, "Mitigating security threats
in tactical networks," in IST Panel Symposium, Military Communication and Networks, 2010, Wroclaw, Poland.

[5] Marti S, Giuli T, Lai K, and Baker M,"Mitigating Routing Misbehavior
in Mobile Ad Hoc Networks,"Proc.ACM MobiCom,pp. 255-265,2000.

[6] Perkins C, Belding-Royer E, Das S, Ad hoc On-demand Distance
Vector (AODV) Routing, Draft-ietf-manet-aodv-11.txt, June 2002
(work in progress).

[7] Weichao Wang, Yi Lu, Bharat Bhargava, "On Security Study of Two
Distance Vector Routing Protocols for Mobile Adhoc Networks", (IEEE) 2003, 0-7695-1893- 1/03.

[8] Alex Hinds, Michael Ngulube, Shaoying Zhu and Hussain Al-Aqrabi,"A Review of Routing Protocols for Mobile Ad-Hoc networks (MANET)," International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.

[9] Komal Joshi and Veena Lomte, "Preventing Flooding Attack in MANET Using Node-to-Node Authentication," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 11, November 2013.

[10] Onkar V. Chandure and Prof. V. T. Gaikwad, "A Mechanism for Recognition & Eradication of Gray Hole Attack using AODV routing protocol in MANET," Onkar V Chandure et al/(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (6), 2011, 2607-2613.