International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.1, No.5, September 2012 DOI:10.15693/ijaist/2012.v1i5.29-33

A New Mechanism for Malicious Detection in MANET

S.Gopinath[1]& M.Vetriselvan[2]
[1,2]Assistant Professor, Department of ECE,
Karpagam Institute of Technology, Coimbatore, India.
,

Abstract:

Mobile Ad-hoc Network (MANET) is a temporary infrastructure less multi-hop wireless network in which the nodes can move arbitrarily. Such networks extend the limited wireless transmission range of each node by multi-hop packet forwarding, thus, well suited for the scenarios in which pre deployed infrastructure support is not available.

It is easy to launch the Denial of Service (DoS) attack by means of malicious node in MANET. The main objective of the work is to detect the malicious node using reputation system. In this system, each node would evaluate its own trust vector parameters about neighbors through monitoring neighbor's pattern of traffic in network. The reputation system based on mobility is integrated in to the existing protocol i.e. DSR. Simulation results shows that the mobility oriented DSR protocol provides better detection efficiency, packet delivery ratio, low delay than DSR protocol.

Keywords-MANET, Malicious, Mobility, packet delivery ratio, Detection efficiency, delay.

I. INTRODUCTION

A. Mobile Ad-hoc Networks

MANET is a self-configuring system of mobile routers linked by wireless links which consequently combine to form an arbitrary topology. Thus, the network's wireless topology may alter rapidly and unpredictably. However, due to the lack of any fixed infrastructure, it becomes complicated to exploit the present routing techniques for network services, and this provides some huge challenges in providing the security of the communication, which is not done effortlessly as the number of demands of network security conflict with the demands of mobile networks, largely due to the nature of the mobile devices e.g. low power consumption, low processing load.

B. Effect of Malicious Node in MANET

In MANET, uncooperative node is malicious node. The nodes belonging to the first category are either faulty and therefore cannot follow a protocol, or are intentionally malicious and try to attack the system. Malicious node causes packet dropping, false routing and etc. Effects of malicious nodes are given below:

- Malicious node reduces the network connectivity in MANETs.
- The result is defragmented networks, isolated nodes, and drastically reduced network performance.
- No intention for energy-saving.
- Launch all kinds of denial-of-service (DoS) attacks by replaying, reordering or/and dropping packets from time to time, and even by sending fake routing messages.

C. Dynamic Source Routing (DSR)

DSR [1] is a source routing protocol. In DSR the source node starts and takes charge of computing the routes. When a node S wants to send messages to node D, it firstly broadcasts a route request (RREQ) which contains the destination and source node's identities. Each intermediate node that receives RREQ will add its identity and rebroadcast it until RREQ reaches a node who knows a route to D or the node D. Then a reply (RREP) will be generated and sent back along the reverse path until S receives RREP. When S sends data packets, it adds the path to the packet's headers and starts stateless forwarding. During route maintenance, S detects the link failures along the path. If it happens, it repairs the broken links. Otherwise, when the source route is completely broken, S will restart a new discovery.

D. Security Challenges in MANET

The nature of MANET makes it vulnerable to attacks. Challenges in MANET securities are discussed briefly [2];

- **Confidentiality:** should preserve certain information which is not to be opened to unauthorized parties.
- **Integrity:** The receiver should believe that the transmitted message is genuine and is never be corrupted.
- **Authentication:** Enables a node to defend the characteristics of the peer node it is communicating, without which an attacker would duplicate a node.
- **Access control** prevents unauthorized use of network services and system resources. Access control is tied to authentication attributes.
- **Availability:** should withstand survivability regardless of Denial-of-Service (DOS) attacks like in physical and media access control layer attacker uses jamming techniques for hinder with communication on physical channel.

II. Related Work

Buchegger and Boudec [3] suggest that despite the fact that networks only function properly if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate. They propose a protocol, called CONFIDANT, which aims at detecting and isolating misbehaving nodes, thus making misbehavior unattractive.

Zapata and Asokan [4] proposed the Secure Ad-hoc On-Demand Distance Vector routing protocol. Through providing security features like integrity, authentication and non-repudiation, it effectively protects the route discovery mechanism. This scheme is based on the assumption that each node should have certified public keys of all nodes in ad hoc network.

K. Sanzgiri et al [5] proposed the Authenticated Routing for Ad-hoc Networks (ARAN) secure routing protocol is an on-demand routing protocol which relies on the use of digital certificates to identifies and defends against malicious actions in the ad-hoc network.

Michiardi and Molva [6] have proposed CORE mechanism that enhances watchdog for monitoring and isolating selfish nodes based on a subjective, indirect and functional reputation. The reputation is calculated based on various types of information on each entity's rate of collaboration. Since there is no incentive for a node to maliciously spread negative information about other nodes, simple denial of service attacks using the collaboration technique itself are prevented.

Naldurg amd Kravets [7] proposed the Security-Aware Ad-hoc Routing (SAR) which deploys a generalized framework for any on-demand secure ad-hoc routing protocol. It uses security information to dynamically control the routing selection process according to routing tables. Nodes at the same trust level must share a secret key.

Li Zhao et.al [8] have proposed MultipAth Routing Single path transmission (MARS) scheme to mitigate adverse effects of misbehavior. This scheme combines multipath routing and single path data transmission with end-to-end feedback mechanism to provide more comprehensive protection against misbehavior from individual or cooperating misbehaving nodes.

Tarag Fahad and Robert Askwith [9] have proposed the new mechanism called Packet Conservation Monitoring Algorithm (PCMA) to detect selfish nodes in the presence of partial dropping when the selfish node does not drop all packets but sends some of them and drops other in MANET.

Bansal and Baker [10] suggests that ad hoc networks rely on the cooperation of the nodes participating in the network to forward packets for each other. A node may decide not to cooperate to save its resources while still using the network to relay its traffic. If too many nodes exhibit this behavior, network performance degrades and cooperating nodes may find themselves unfairly loaded.

III. OVERVIEW OF THE PROPOSED MECHANISM

We propose a Mobility Oriented Reputation System (MORS) in MANETs without using any centralized infrastructure. It uses trust table to favor packet forwarding by maintaining a trust vector for each node. Each intermediate node marks the packets by adding its recommendation about the neighborhood node, experience and knowledge towards the destination node. The destination node verifies the recommendation about nodes experience and knowledge. Once the destination node's verification is completed, then checks the trust vector. If the recommendation, experience and knowledge are verified, the trust vector is incremented, otherwise it is decremented. If the trust vector value falls below a trust vector threshold value, the corresponding the intermediate node is marked as malicious node.

IV. Efficient Misbehavior Node Detection System

A. Mobility Oriented Reputation System (MORS)

In our proposed system, by calculating the nodes trust vector values, the source node can be able to select the more trusted routes rather than selecting the shorter routes. Our system marks and isolates the malicious nodes from participating in the network. So the potential damage caused by the malicious is significantly reduced.

Let $\{Tv_1, Tv2\ldots\}$ be the initial trust vectors of the nodes $\{n_1, n2\ldots\}$ along the route R1 from a source S to the destination D.

Node does not have any information about the reliability of its neighbors in the beginning; nodes can neither be fully trusted nor be fully distrusted. When a source S wants to establish a route to the destination D, it sends route request (RREQ) packets.

When the destination D receives the accumulated RREQ message, it measures the number of packets received Prec. Then it constructs a route on Prec with the key shared by the sender and the destination. The RREP contains the source and destination ids, the route of Prec, the accumulated route from the RREQ, which are digitally signed by the destination. The RREP is sent towards the source on the reverse route R1.

The intermediate node then verifies the digital signature of the destination node stored in the RREP packet, is valid. If the verification fails, then the RREP packet is dropped. Otherwise, it is signed by the intermediate node and forwarded to the next node in the reverse route.

When the source S receives the RREP packet, if first verifies that the first id of the route stored by the RREP is its neighbor. If it is true, then it verifies all the digital signatures of the intermediate nodes, in the RREP packet. If all these verifications are successful, then the trust counter values of the nodes are incremented as

$$Tv_i = Tv_i + \alpha_1 \quad (1)$$

If the verification is failed, then

$$Tv_i = Tv_i - \alpha_1 \quad (2)$$

Where α_1 is the step value, which can be assigned a small fractional value during simulations. After this verification stage, the source S check the digital signature values DS of the nodes n_i.

The digital signature includes recommendation about the neighbor nodes, nodes knowledge and experience successfully.

Evaluating the recommendation is given by R_B^A which is node A's evaluation to node B by collecting recommendations

$$R_B^A = \frac{\sum_{v \in \gamma} Trust\ Vector\ of\ node\ A\ to\ C * Trust\ vector\ of\ node\ C\ to\ B}{Trust\ Vector\ of\ node\ A\ to\ C}$$

γ is a group of recommenders.

Nodes knowledge can be defined by,

$= (1-p_{A,B}) * (1-p_{B,A})$

Probability can be defined by which is node A's evaluation to node B by directly determining MAC layer link quality between node A and node B on the physical layer.

$p_{A,B}$ is packet loss probability from node A to node B, while $p_{B,A}$ is packet loss probability from node B to node A.

Nodes experience E_B^A is given by,

$$\frac{Outcoming\ packets\ from\ node\ B - Packets\ from\ node\ B\ to\ A}{Outcoming\ packets\ from\ node\ B - Packets\ from\ node\ B\ to\ B},$$

P_B^A

For any node n_k if $DS_k < DS_{min}$, where DS_{min} is the minimum threshold value, its trust vector value is further decremented as

$$Tv_i = Tv_i - \alpha_2 \quad (5)$$

For all the other nodes with $DS_k > DS_{min}$, the trust counter values are further incremented as

$$Tv_i = Tv_i + \alpha_2 \quad (6)$$

Where α_2 is another step value with $\alpha_2 < \alpha_1$.

For a node n_k, if $Tv_k < Tv_{thr}$, where Tv_{thr} is the trust threshold vector value, then that node is considered and marked as malicious. If the source does not get the RREP packet or RERR packet for a time period of t seconds, it will be considered as a node failure or link failure. Then the route discovery process is initiated by the source again. The same procedure is repeated for the other routes R2, R3 etc and either a route without a malicious node or with least number of malicious nodes, is selected as the reliable route.

V.TRUST INTEGRATION IN DSR PROTOCOL

In trust vector evaluation, how many out-coming packets can be measured that the immediate neighboring node had been sincerely sent. Participation of the nodes in the packet forwarding is monitored. So nodes are placed in the immoral mode all the time whether a node transmits control packets or data packets. When it eavesdrops its immediate neighbor nodes forwarding the packet, it should first checks the integrity of the packet in order to make sure the packet had not been modified by other malicious nodes. Neighbor node should be incremented if it passes integrity test. However if the integrity test fails or the neighbor node refuse to cooperate to forward packets it supposed to, its corresponding forwarding counter would not change. After a period of time, its experience value would be extremely low as a result of malevolent behavior. The mobility oriented reputation system is integrated in to DSR routing protocol. This mobility oriented DSR is compared with DSR protocol.

VI. PERFORMANCE EVALUATION

A. Simulation Model and Parameters

We use NS2 to simulate our proposed algorithm. In our simulation, 101 mobile nodes move in a 1000 meter x 1000 meter square region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 100 meters. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in table 1

No. of Nodes	100
Area Size	1000 X 1000
Mac	802.11
Radio Range	100m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	80 bytes
Mobility Model	Random Way Point

B. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Detection Efficiency: The ratio of detected malicious nodes to the total number of nodes.

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

Average Packet Delivery Ratio: It is the ratio of the number .of packets received successfully and the total number of packets transmitted.

The simulation results are presented in the next part. We compare our mobility oriented DSR with the DSR protocol in presence of malicious node environment.

C. Results

Nodes actual behaviors comply with the Bernoulli trial, which means that the probability that a node acts good is predetermined. If a node acts well for less than 40 percent of the

interactions, it is considered as a malicious node. The default percentage of malicious node in the network is 20 percent.

In our First experiment, we vary the no. of malicious nodes as 20, 30 up to 100.

Figure 1 show the results of detection efficiency for the nodes 20, 30….100 scenarios. Clearly our MODSR scheme achieves more detection rate than the DSR protocol and certainty reputation system.

Figure 2 shows the results of No. of Nodes Vs overhead. From the results, we can see that MODSR scheme achieves less overhead than the DSR protocol and certainty reputation system.

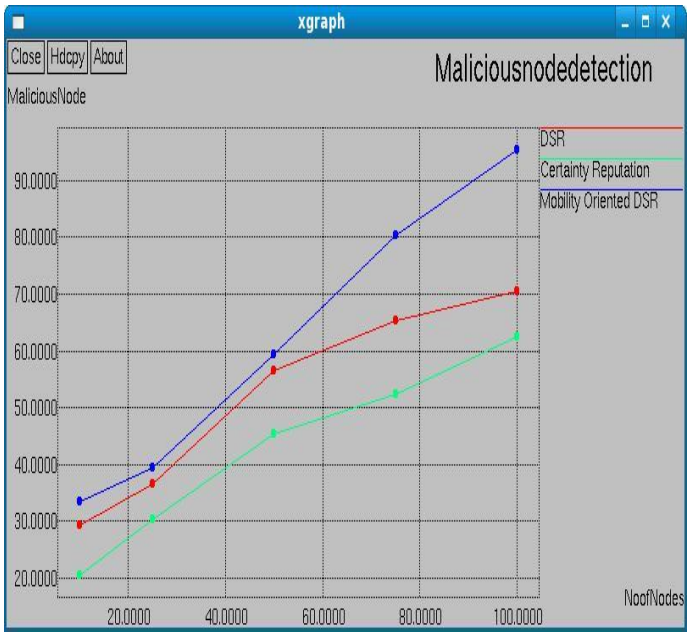

Figure 1. Detection Efficiency

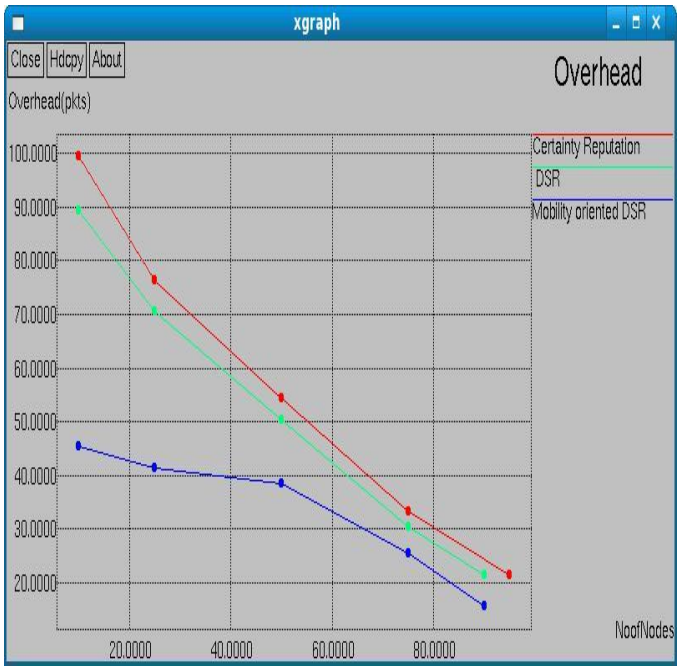

Figure 2. No of nodes Vs Overhead

In our Second experiment, we vary the speed as 20, 40,60. 80,100.

Figure 3.No of nodes Vs Packet Delivery Ratio

Figure 4. No of nodes Vs Delay

Figure 3 show the results of packet delivery ratio for the No. of nodes. Clearly our MODSR achieves more packet delivery ratio than the DSR protocol and certainty reputation system.

Figure 4 shows the results of No of nodes Vs delay. From the results, we can see that MODSR scheme has less delay than the DSR protocol and certainty reputation system.

VII. Conclusion

It is easy to deploy malicious node to impersonate another node in MANET. Mobile ad hoc network has no clear line of defense, so, it is accessible to both legitimate network users and malicious nodes. In this paper, we have developed a mobility oriented reputation system which attains trust convergence and authentication to the mobile nodes. In the first phase of the scheme, detection of the malicious node is achieved. It uses trust table to favor packet forwarding by maintaining a trust vector for each node. A node is punished or rewarded by decreasing or increasing the trust counter. A node is reprimanded or satisfied by decreasing or increasing the trust vector value. If the trust vector value falls below a trust vector threshold value, the corresponding the intermediate node is marked as malicious. By simulation results, we have shown that the mobility oriented reputation system achieves better detection efficiency, good packet delivery ratio while attaining low delay.

References

[1]. P Narayan, V R. Syrotiuk,"Evaluation of the AODV and DSR Routing Protocols Using the MERIT Tool", In In proceeding or ADHOC-NOW 2004, pp. 25-36.

[2]. Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless Network Security, Springer Book, ISBN: 978-0-387-28040-0, pp. 103--135, 2007.

[3]. S. Buchegger and J. Boudec, "Performance Analysis of the Confidant Protocol," Proc. Int'l Symp. Mobile Ad Hoc Networking and Computing, 2002.

[4]. M. Guerrero Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. ACM Workshop on Wireless Security (WiSe), ACM Press, 2002, pp. 1–10.

[5]. K. Sanzgiri et al., "A Secure Routing Protocol for Ad Hoc Networks," Proc. 10th IEEE Int'l Conf. Network Protocols (ICNP '02), IEEE Press, 2002, pp. 78–87.

[6]. P. Michiardi and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm.and Multimedia Security, 2002.

[7]. Yi, S., Naldurg, P., Kravets, R., "Security aware ad-hoc routing for wireless networks," Proc. of the 2nd ACM International Symposium on Mobile ad hoc networking and computing (MobiHoc'01), 2001, pp. 299-302.

[8]. Li Zhao and José G. Delgado-Frias, "MARS: Misbehavior Detection in Ad Hoc Networks", in Proceedings of IEEE GLOBECOM 2007,pp. 941-945.

[9]. Tarag Fahad and Robert Askwith "A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks", in proceedings of the 7th Annual Post Graduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, June 2006.

[10]. S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad Hoc Networks," Technical Report cs.NI/0307012, Stanford Univ., 2003.