International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:8, 2009

Performance Analysis of Flooding Attack Prevention Algorithm in MANETs

Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao

***Abstract*—**The lack of any centralized infrastructure in mobile ad hoc networks (MANET) is one of the greatest security concerns in the deployment of wireless networks. Thus communication in MANET functions properly only if the participating nodes cooperate in routing without any malicious intention. However, some of the nodes may be malicious in their behavior, by indulging in flooding attacks on their neighbors. Some others may act malicious by launching active security attacks like denial of service. This paper addresses few related works done on trust evaluation and establishment in ad hoc networks. Related works on flooding attack prevention are reviewed. A new trust approach based on the extent of friendship between the nodes is proposed which makes the nodes to co-operate and prevent flooding attacks in an ad hoc environment**.** The performance of the trust algorithm is tested in an ad hoc network implementing the Ad hoc On-demand Distance Vector (AODV) protocol.

***Keywords*—** AODV, Flooding, MANETs, trust estimation

I. Introduction

AD HOC networks are simple peer-to-peer networks, self-organized with no fixed infrastructure. This leads to new vulnerabilities which are not known in wired networks. The wireless links and dynamic topology definitely gives flexibility in installation. But, at the same time, security is a major concern in these networks. The wireless channels are vulnerable to various security attacks [1]. Some of the ad hoc nodes may be victimized in the network by malicious nodes and may indulge in various denial-of-service attacks [2]. Many security and trust based algorithms are proposed in [2,3]. The lack of security frameworks in these networks are one of the major concerns in their large scale deployments. Most of the reactive protocols are prone to flooding attacks during their route discovery process. A malicious node may actively involve in the flooding attack by repeatedly sending RREQ or garbage DATA packets to different destinations some of which never exists. A neighboring victim node may drain its resources like battery power, processing time by involving itself in the routing traffic.

Our proposal is an initiative towards developing a foolproof security model which can detect and prevent a good subset of security attacks possible in an ad hoc environment.

This paper briefs about the flooding attacks by neighboring nodes and strategies to prevent this attack. The rest of the paper is organized as follows. Section 2 briefs about the security issues and the related works done on the trust evaluation and establishment in ad hoc networks. Specifically, relevant works done on resisting flooding attacks are addressed. Section 3 describes the algorithm for preventing the flooding attacks which is based on extent of friendship between the nodes. Section 4 analyzes the performance issues of the algorithm over AODV protocol. Section 5 concludes by pointing to future work.

II. Related Works

The lack of trusted environment in an ad hoc network results in many security lapses. This is considered as one of the major concerns in the large scale deployment of ad hoc networks [4]. Many trust establishment algorithms [5, 6, 7] have been developed which addresses few of the security attacks possible in an ad hoc network. The participating nodes should know in advance regarding the type of security attack in the network and run the corresponding algorithm to detect the misbehaving nodes in the network. The Secure Ad hoc On-demand Distance Vector (SAODV) routing protocol presented in [8] is based on public key infrastructure which is not suitable for an ad hoc environment where there is no centralized infrastructure. Some of the cryptographic protocol schemes [9,10] presented clearly have the overheads associated with the secure routing at all times. The battery power and computational overheads assume great importance in a resource constraint MANET environment.

Resisting flooding attacks in ad hoc networks presented in [11] describes two flooding attacks: Route Request (RREQ) and Data flooding attack. In RREQ flooding attack the attacker selects many IP addresses which are not in the network or select random IP addresses depending on knowledge about scope of the IP address in the network. Using neighborhood suppression, a single threshold is set up for all neighboring nodes In Data flooding attack the attack node first sets up the path to all the nodes and send useless packets. The given solution is that the data packets are identified in application layer and later path cutoff is initiated. Similar solutions are proposed in [12] where a rate-limitation component is added in each node. This component monitors the threshold limit of request packets sent by the neighboring

Revathi Venkataraman and M. Pushpalatha are working in Department of Computer Science and Engg, SRM University, Chennai, India (phone: 91-44-27452270; e-mail: revathi@cse.srmuniv.ac.in, lathamarudappa @yahoo. co. in).

T. Rama Rao is with Telecommunication Engineering department, SRM University, Chennai, India (e-mail: ramarao@ieee.org).

nodes and accordingly, drops the packets if the limit is exceeded. Data Flooding is not addressed in the work.

The flooding attacks prevention algorithm over DSR protocol is proposed in [13] where the neighboring nodes are categorized as *strangers*, *acquaintances* and *friends* with different thresholds and provide a cutoff once the threshold is reached by using the extended DSR protocol [14]. A generalized trust model and evaluation metric as proposed in [15], is integrated into our extended DSR model. This paper describes the flooding attacks prevention algorithm modified to run over AODV protocol and presents the simulation analysis of the work.

III. Proposal for Flooding Attack Prevention

All the nodes in an ad hoc network are categorized as *friends*, *acquaintances* or *strangers* based on their relationships with their neighboring nodes. During network initiation all nodes will be *strangers* to each other. A *trust estimator* is used in each node to evaluate the trust level of its neighboring nodes. The trust level is a function of various parameters like length of the association, ratio of the number of packets forwarded successfully by the neighbor to the total number of packets sent to that neighbor, ratio of number of packets received intact from the neighbor to the total number of received packets from that node, average time taken to respond to a route request etc. Accordingly, the neighbors are categorized into *friends* (most trusted), *acquaintances* (trusted) and *strangers* (not trusted).

In an ad hoc network, the relationship of a node *i* to its neighbor node *j* can be any of the following types

(i) Node i is a *stranger* (S) to neighbor node j:

Node i have never sent/received messages to/from node j. Their trust levels between each other will be very low. Any new node entering ad hoc network will be a stranger to all its neighbors. There are high chances of malicious behavior from stranger nodes.

(ii) Node i is an *acquaintance* (A) to neighbor node j:

Node i have sent/received few messages from node j. Their mutual trust level is neither too low nor too high to be reliable. The chances of malicious behavior will have to be observed.

(iii) Node i is a *friend* (F) to neighbor node j:

Note i sent/received plenty of messages to/from node j. The trust levels between them are reasonably high. Probability of misbehaving nodes may be very less.

The above relationships are computed by each node and a friendship table is maintained for the neighbors. Fig. 1 shows the relationship of N4 with its neighbors. The corresponding friendship table maintained in N4 is given in Table I. The threshold trust level for a stranger node to become an acquaintance to its neighbor is represented by T_{acq} and the threshold trust level for an acquaintance node to become a friend of its neighbor is denoted by T_{fri}.

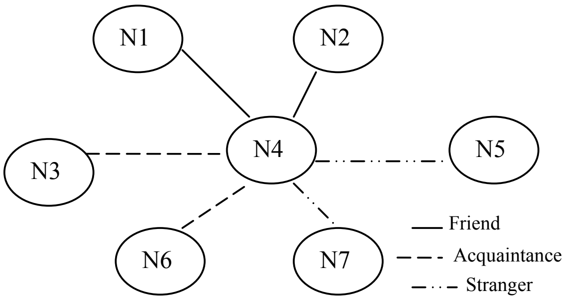

Fig. 1 Trust Relationship of a node in an ad hoc network

The relationships are represented as:

$R(n_i \rightarrow n_j) = F$ when $T \geq T_{fri}$
$R(n_i \rightarrow n_j) = A$ when $T_{acq} \leq T < T_{fri}$
$R(n_i \rightarrow n_j) = S$ when $0 < T < T_{acq}$

During route discovery phase of the DSR protocol, the extended system also computes the aggregate trust along different paths to the destination by the "path semiring" algorithm as proposed in [1]. From this, the most trusted path between the source and the destination is found out before establishing the data transfer. The segregation of the neighboring nodes into *friends*, *acquaintances* and *strangers* is the outcome of the direct evaluation of trust.

TABLE I
Friendship Table for Node (N4) in Fig. 1

Neighbors	Relationship
N1	F
N2	F
N3	A
N5	S
N6	A
N7	S

To prevent RREQ flooding, the threshold level is set for the maximum number of RREQ packets a node can receive from its neighbors. To prevent DATA flooding, the intermediate node assigns a threshold value for the maximum number of data packets it can receive from its neighbors. If X_{rs}, X_{ra}, X_{rf} be the RREQ flooding threshold for a stranger, acquaintance and friend node respectively, $X_{rf} > X_{ra} > X_{rs}$. If Y_{rs}, Y_{ra}, Y_{rf} be the DATA flooding threshold for a stranger, acquaintance and friend node respectively then $Y_{rf} > Y_{ra} > Y_{rs}$. If the specified threshold level is reached, further RREQ packets from the initiating node are ignored and dropped. Thus, flooding is prevented in the routing table.

TABLE II
ALGORITHM FOR RREQ FLOODING

```
Begin
if an intermediate node receives RREQ flooding packet from node 'i' then
    if node 'i' is a friend and Z[i] = 0 then
        increment X[i]
        if X[i] > $X_{rf}$
            drop the RREQ packet and set Z[i] = 1
        else
            forward the RREQ packet
    if node 'i' is an acquaintance and Z[i] = 0 then
        increment X[i]
        if X[i] > $X_{ra}$
            drop the RREQ packet and set Z[i] = 1
        else
            forward the RREQ packet
    if node 'i' is an stranger and Z[i] = 0 then
        increment X[i]
        if X[i] > $X_{rs}$
            drop the RREQ packet and set Z[i] = 1
        else
            forward the RREQ packet
End
```

Let X[i] denotes the number of packets delivered from neighboring node i, where $1 \leq i \leq n$. X_{rf}, X_{ra} and X_{rs} are the threshold values set for *friends*, *acquaintances* and *strangers*. Let Z[i] is a Boolean array to activate or stop the prevention algorithm. The algorithm for preventing RREQ flooding is as given in Table II. The algorithm to prevent DATA flooding is similar to the algorithm discussed in Table II. The threshold values for DATA flooding can be set as per the requirements of the application software.

IV. SIMULATION ANALYSIS

Simulations are carried out to test the performance of the flooding attack prevention algorithm over AODV protocol. Compromised nodes are introduced into the network which involve in RREQ flooding. The trust levels for neighbors are determined by the nodes. Fig. 2 shows the routing traffic sent by a malicious node in a compromised network. Fig. 3 illustrates the routing traffic received by a victim node which is nearer to a malicious node. The volume of routing information received by the victim node will deprive it of its resources. Most of the victim nodes energy will be exhausted by listening to the routing traffic sent by the malicious neighbor.

The nodes are made to move in a random fashion in a 500 X 500m area in the simulation setup. Each node starts at a random position and randomly moves to another position with a chosen velocity ranging from 0 m/s to 20 m/s. Random Waypoint model is chosen as the movement pattern. To evaluate the performance of the Flooding Attack Prevention algorithm, WLAN throughput and delay in the network are considered. In the default setup, the nodes communicate using the AODV protocol which shows the degradation in throughput of the network and increased delay in the presence of malicious nodes. With the implementation of flooding attack prevention algorithm over AODV, the flooding attacks are constrained and this results in increased throughput and reduced delay.

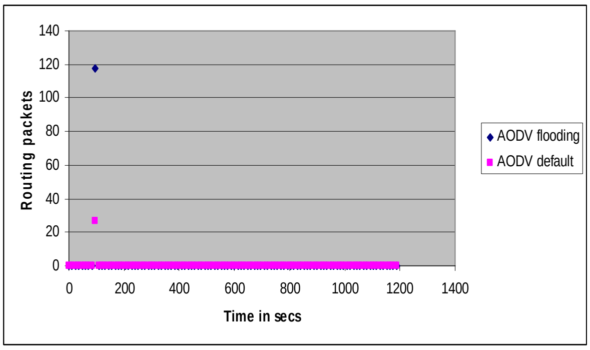

Fig. 2 Routing Traffic sent by a malicious node (bits/sec)

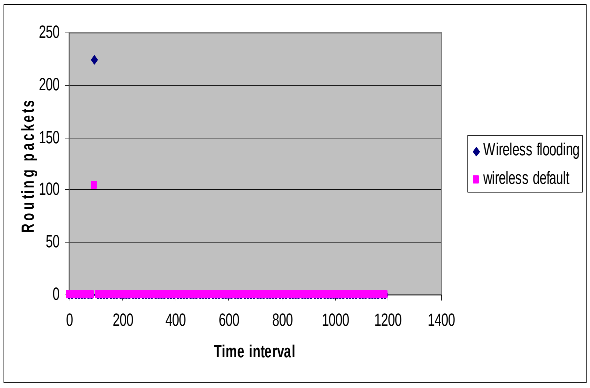

Fig. 3 Routing Traffic received by a victim node (bits/sec)

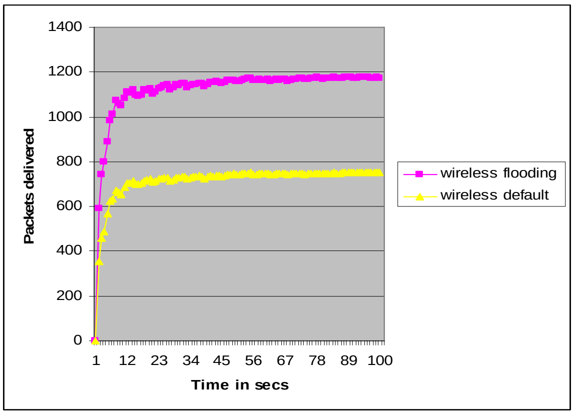

Fig. 4 Wireless LAN Throughput (bits/sec)

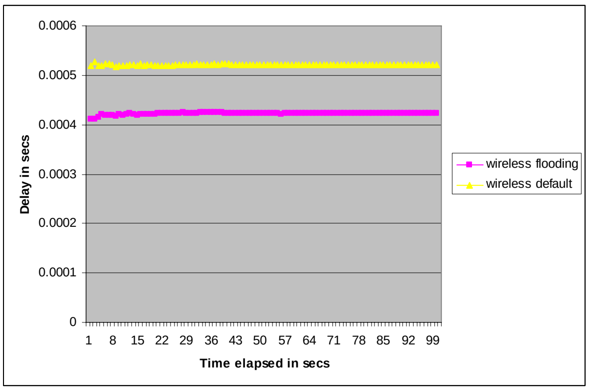

Fig. 5 WLAN delay

Fig. 4 shows the increase in the throughput of the network improvised with the prevention algorithm. All the nodes in the network monitor the threshold values of their respective neighbors. If the neighbors exceed their limit in sending the RREQ packet, they are immediately destroyed. Hence the neighboring nodes do not waste their energy, involving in superfluous traffic information. Their resources are conserved. This results in the overall improvement in the throughput of the network. Additionally, Fig. 5 shows the decrease in the delay of packet traffic in the network due to reduction in the volume of routing traffic by malicious nodes. The unnecessary traffic in the network is reduced and hence the nodes are able to process the data traffic and send to the destination in less time.

V. Conclusion

Mobile ad hoc networks exhibit new vulnerabilities to malicious attacks or denial of cooperation. This paper addresses related works on security issues and trust establishment schemes. A proposal to effectively prevent flooding attack using extended AODV Protocol is discussed. A better understanding and modeling of the security attacks is needed in MANETs if efficient secure routing algorithms are to be built in the network. Our future work will include simulation and performance analysis of our proposed flooding attack prevention and to develop comprehensive models for security attacks and a trustworthy security framework against all possible security attacks in an ad hoc network.

Acknowledgment

The authors wish to acknowledge the support of the SRM University, Chennai, India to carryout this research work.

References

[1] Amitabh Mishra, "Security and Quality of Service in Ad hoc Wireless Networks,"pp. 42-57, Cambridge University Press, 2008.

[2] C.Siva Ram Moorthy, B.S. Manoj: Ad hoc Wireless Networks Architectures and Protocols, Prentice Hall, 2004.

[3] Revathi Venkataraman, M.Pushpalatha and T.Rama Rao, "A Graph-theoretic algorithm for detection of multiple wormhole attacks in mobile ad hoc networks". International Journal of Recent Trends in Engineering, Issue 1, Vol.1, May 2009. (Accepted for publication).

[4] Imrich Chlamtac, Marco Conti, Jennifer J.-N. Liu, Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks I(2003)pp. 13-64, Elseiver publications.

[5] Jie Li and Jien Kato, Future Trust Management Framework for Mobile Ad hoc Networks. IEEE Communications Magazine, April 2008

[6] Y.Sun *et al*., Defense of trust management vulnerabilities in distributed networks, IEEE Communications Magazine, February 2008.

[7] Y.Sun et al., Information Theoretic Framework of Trust Modeling and Evaluation for ad hoc networks. IEEE JSAC, vol.24, no.2, Feb.2006.

[8] Manel Guerrero Zapata, Secure ad hoc on-demand distance vector routing, ACM SIGMOBILE Mobile Computing and Communications Review, v.6 n.3, July 2002 [doi>10.1145/581291.581312]

[9] Panagiotis Papadimitratos and Zygmunt J.Haas, Secure Data Communication in Mobile Ad hoc Networks, IEEE JSAC, Vol.24, No.2, February 2006.

[10] P.Papadimitratos and Z. Hass and P.Samar. The Secure Routing Protocol (SRP) for Ad hoc Networks. Draft-papadimitratos-secure-routing-protocol-00.txt, Dec.2002.

[11] Yi Ping, Hou Yafei, Bong Yiping, Zhang Shiyong & Dui Zhoulin, Flooding Attacks and defence in Ad hoc networks. Journal of Systems Engineering and Electronics, VoL. 17, No. 2, pp. 410- 416, 2006.

[12] Venkat Balakrishnan *et al.* Mitigating Flooding attacks in Mobile Ad hoc Networks Supporting Anonymous Communications. In proceedings of the 2nd International Conference on Wireless and Ultra Wideband Communications (Auswireless 2007).

[13] Revathi Venkataraman, M.Pushpalatha: "Prevention of Flooding Attacks in Mobile Ad hoc Networks" In the proceedings of International Conference on Advances in Computing, Communication and Control, pp. 525-529. January 2009.

[14] Revathi Venkataraman, M. Pushpalatha: Security in Ad Hoc Networks: An extension of dynamic Source Routing in Mobile Ad Hoc Networks. In proceedings of the 10th IEEE International Conference on Communication Systems, Singapore, 2006.

[15] George Theodorakopoulos and John S. Baras, On Trust Models and Trust Evaluation Metrics for Ad Hoc Networks. *IEEE JSAC*, Vol.24. No.2, February 2006.