Volume 2, No. 3, May-June 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

New Approach Secure AODV in Mobile Ad-hoc Network

Akansha Gupta*
Computer Science & Engineering Department
R.K.D.F, Bhopal,
M.P., India.
akanshagpt4@gmail.com

Rajdeep Singh
Computer Science & Engineering Department
R.K.D.F, Bhopal,
M.P., India.

Nirlesh Sharma
Computer Science & Engineering Department
R.K.D.F, Bhopal,
M.P., India.

Abstract: - In Ad hoc On Demand Vector (AODV) routing protocol for MANET (Mobile Ad hoc Networks), malicious nodes can easily disrupt the communication because of inherent limitations. A malicious node that is not part of any route may launch Denial of Service (DoS) Attack. Also, once a route is formed, any node in the route may turn malicious and may refrain from forwarding packets, modify them before forwarding or may even forward to an incorrect intermediate node. Such malicious activities by a misbehaving node cannot be checked for in pure AODV protocol. In this paper we proposed a new approach secure ad-hoc on demand distance vector in MANET using implement the prevention technique of flooding attack (Denial of services). In our simulation, the results show that SAODV is still efficient in discovering secure routes compared with normal AODV protocol.

Keywords- MANET, AODV, Flooding Attack

1. INTRODUCTION

There are major issues and sub-issues involving in MANET such as routing; multicasting/broadcasting, location service, clustering mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance, Qos/multimedia and standards/products. Currently, the routing, power management, bandwidth management, radio interference and security are hot topics in MANET research. Although in this thesis we only focus on AODV routing protocol and its security issues in MANET [1].

In AODV, a communication link is established between the source and the destination by a route discovery procedure initiated by the source. How-ever, AODV is subject to various malicious activities before the route is formed as well as after its establishment. AODV routing protocol provides control messages for route discovery and subsequent route maintenance but cannot guard against their flooding, deliberate dropping or malicious modification. Before a route is established, a malicious node can flood the network with false control packets, such as RREQs (Route Requests), congesting the network leading to DoS attacks.

Once a route is formed, any intermediate node in the route, which turns malicious can drop packets, modify them before forwarding or tunnel them. Our scheme is implement the prevention technique of flooding attack (Denial of services) addresses these malicious activities and detects the node, which is misbehaving both prior to route formation (during route discovery) and after its establishment (during communication). Our scheme is reported to quantify the effectiveness of the proposed scheme; malicious activities were simulated in the mobile environment [1] and [2].

II. BACKGROUND

A. Routing in ad-hoc Network

a. Temporally-Ordered Routing Algorithm (TORA)

TORA can work in environment where mobility is highly dynamic. TORA's algorithm concept is link reversal, which has the feature of loop-free and adaptive distributed routing. It provides multiple routes for any required source/destination pair and that's why it falls in source-initiated category. Localization of control message is the key design of TORA, which adopts topological changes very quickly [3].

b. Authenticated Routing for Ad-hoc Network (ARAN)

ARAN main feature is to find and protect from the misbehaving nodes from third party and peers environment. To do so in an Ad-Hoc network ARAN introduces a minimal security policy to integrate, authenticate and non-repudiation of messages. While using ARAN one has to pay less performance cost to achieve high security [5].

c. Secure Efficient Ad-hoc Distance Vector (SEAD)

SEAD is an extended version of DSDV. In order to maintain less CPU processing and to be suitable for Denial of Service from attackers some efficient one-way has been implemented in SEAD rather than asymmetric cryptographic operation in DSDV. SEAD is robust against attackers in all scenarios where it has been tested so for [6].

d. Zone Routing Protocol (ZRP)

It is not a separate protocol instead it's a hybrid solution having the advantages of both reactive and proactive schemes. Proactive scheme is used for the discovery of local neighborhoods and for communication between neighborhoods reactive scheme is used. In MANET the

changes in topology, which took place far from neighbors, does not affect the vicinity of a node as most of the communication in MANET took place within the neighbors [3].

e. Dynamic Source Routing Protocol (DSRP)

The Dynamic Source Routing Protocol is a source-routed on-demand routing protocol. A node maintains route caches containing the source routes that it is aware of. The node updates entries in the route cache as and when it learns about new routes. The two major phases of the protocol are: route discovery and route maintenance. When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the packet. But if the node does not have such a route, then it initiates the route discovery process by broadcasting a route request packet. The route request packet contains the address of the source and the destination, and a unique identification number. Each intermediate node checks whether it knows of a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors. To limit the number of route requests propagated, a node processes the route request packet only if it has not already seen the packet and it's address is not present in the route record of the packet. A route reply is generated when either the destination or an intermediate node with current information about the destination receives the route request packet. A route request packet reaching such a node already contains, in its route record, the sequence of hops taken from the source to this node [1].

B. Related Works

Security issues with routing in general have been addressed by several researchers. And, lately, some work has been done to secure ad hoc networks by using misbehavior detection schemes. This approach has two main problems: first, it is quite likely that it will be not feasible to detect several kinds of misbehaving (especially because it is very hard to distinguish misbehaving from transmission failures and other kind of failures); and second, it has no real means to guarantee the integrity and authentication of the routing messages.

In recent proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server. In ARAN, every node that forwards a route discovery or a route reply message must also sign it, (which is very computing power consuming and causes the size of the routing messages to increase at each hop), whereas the proposal presented here only require originators to sign the message. In addition, it is prone to reply attacks using error messages unless the nodes have time synchronization [7].

In previous proposed a protocol (SRP) that can be applied to several existing routing protocols (in particular DSR and IERP. SRP requires that, for every route discovery, source and destination must have a security association between them. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected, and any malicious node can just forge error messages with other nodes as source [2] and [8].

The lack of security frameworks in these networks are one of the major concerns in their large scale deployments. Many trust establishment algorithms 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 DSR protocol for dependable routing as presented the possibility of flooding and sinkhole attacks in the network. Some of the cryptographic protocol schemes 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 [3] and [9].

Resisting flooding attacks in ad hoc networks 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. A single threshold is set up for all the neighbor nodes. The given solution is neighbor suppression. 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. After the data flooding has occurred, the steps are being initiated to curb the flooding attack. Similar solutions are proposed where a rate-limitation component is added in each node. This component monitors the threshold limit of request packets sent by the neighboring nodes and accordingly, drops the packets if the limit is exceeded. Data Flooding is not addressed in the work [4] and [10].

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

III. PROPOSED TECHNIQUE

In our scheme we have categorized the neighboring nodes as strangers, acquaintances and friends with different thresholds and provide a cutoff once the threshold is reached by using the extended AODV protocol. Simulation and analysis is to be carried out wherein the network model is to be test run with different types of attacks. We have modified the extended AODV to prevent the flooding attack by the neighboring nodes.

In this paper we propose a detection feature, RREQ packet rate to detect high rate flooding attack.

To acquire our detection feature, each node counts the number of RREQ packets ($N_{i,j}$) belonging to a certain RREQ flow j seen in sampling interval Δti. At the end of Δt_i, this node can calculate the RREQ packet rate ($R_{i,j}$) of flow j, $R_{i,j} = N_{i,j} / \Delta t_i$. If this node *sees* k flows in Δti, the average RREQ packet rate, $avgRate_i$, of k *f*lows in Δt_i is calculated by Equation 1, and the standard deviation, $stdRate_i$, is given by Equation 2.

$$avgRatei = \sum_{j=1}^{k} Ri,j \Big/ k \quad \text{..... (1)}$$

$$stdRatei = \sqrt{\sum_{j=1}^{k} (Ri,j - avgRatei)^2} \Big/ k-1 \quad \text{... (2)}$$

$$\mathbf{T_{Ratei}} = avgRate_i + 3.\ stdRate_i \quad \text{..... (3)}$$

The high rate flooding attack can be identified by the following rule: if a node's RREQ packet rate *Ri,j* counted in Δti exceeds a given threshold *TRatei* , this node is confirmed

as a high rate flooding attacker at Δti. The adaptive detection threshold is given by equation 3.

We model the flooding attack detection as the sequential change point detection problem. Then, we propose to apply the non-parametric algorithm on our detection features to perform the flooding attack identification.

A. Sequential Change Point Detection

As described before, RREQ traffic in MANETs is a complex stochastic process. The flooding attack can result in abrupt changes of certain RREQ traffic feature. Currently, two approaches are widely being used in the abrupt change detection:

a. Fixed-size batch detection and sequential change point detection. The fixed-size batch detection is an on-line approach that first collects sampled data over a fixed time interval (one hour or one day). Then, it makes a decision of homogeneity or a change point. The sequential change point detection approach monitors and detects changes of detection variables on the run (on-line). Compared to the fixed-size batch detection approach, the sequential change point detection has advantages of quick detection and light requirements of memory and computation, which suit well the MANET environment. Thus, we decide to model the detection of flooding attack as a sequential change point problem.

Originally arising from statistical quality control, now the sequential change point detection has many other important applications, including reliability, signal detection, fault detection, surveillance, and finance and so on. Its objective is to determine if the observed variable series is statistically homogeneous, and if not, to find the point in time when the change happens. We, in this work, choose to apply the algorithm on random sequence $\rightarrow Xi$ to identify its changes.

The basic idea behind our method is as follows: if any change occurs on the observed statistical process, the probability distribution of such process will change correspondingly. We decide to adopt the non-parametric method to perform the change detection. The reasons are given as follows.

[i] The parametric version of our algorithm requires a prior knowledge of statistical model for the random sequence $\{Xi\}$. However, due to the dynamic and complicated nature of MANETs, acquiring an accurate statistical model of the RREQ traffic still remains an open problem, which is beyond the scope of this thesis.

[ii] The non-parametric method, on the other hand, does not need such prior knowledge of statistical model. Instead, it monitors and records the mean value of the random sequence under a normal scenario. Then, it accumulates those values of random variables that are significantly higher than the mean value. Once these accumulated values exceed a given threshold, a change (or attack) is said to be detected.

According to the non-parametric algorithm has a requirement for the applied random sequence $\{Xi\}$: the mean of $\{Xi\}$, α, is negative in normal scenario and becomes positive when a change (attack) takes place. To satisfy this requirement, we transform $\{Xi\}$ to $\{Zi\}$ by equation (4).

$$Zi = Xi - \beta \quad \rightarrow\rightarrow Equation \quad (4)$$

where $\beta = \alpha + |a|$, and a is the mean of $\{Zi\}$. a is negative during normal conditions, and becomes positive when a change occurs. Then we define the third variable $\{Yi\}$ using equation (5)

$$Yi = (Yi\text{-}1 + Zi)^{+},\ Y0 = 0 \quad \rightarrow\rightarrow \text{Equation} \quad (5)$$

where $X+$ is equal to X if $X > 0$, and 0 otherwise. From the definition of$\{Zi\}$, we can see that: (1) $\{Zi\}$ is negative in normal scenario; (2) When attack is launched, $\{Zi\}$ will become positive and large, i.e. $h + a > 0$. Thus, these positive values of $\{Zi\}$ are accumulated by $\{Yi\}$, and negative values are dropped. A large value of $\{Yi\}$ strongly indicates an attack. The decision function can be described as follows.

$d_T(Yi) = 0$; if Yi < T

$d_T(Yi) = 1$; if Yi >= T

T is the threshold for the attack detection and $d_T(Yi)$ represents the decision at time i. If $Yi \geq T$, $d_T(Yi)$ is `1', which indicates the detection of a change (attack). If $Yi$ is less than $T$, $d_T(Yi)$ is `0', meaning there is no change. The algorithm is summarized as follows:

```
input: Original values of detection feature {Xi} , T
Output: Detection decision dT (Yi)
→foreach Input {Xi} do
→Zi = Xi - β;
→ Yi = (Yi-1 + Zi) +;
→ if Yi < T then
→ dT (Yi) = 0;
→ end
→ else
→dT (Yi) = 1;
→ end
→ end
→ return dT (Yi);
```

We designed flow based detection features to characterize the flooding attack forms respectively.

We are able to handle all attack variations in the flooding attack spectrum. We modeled the detection of flooding attacks into the sequential change point detection problem, and proposed to apply the above algorithm on those detection features to identify the occurrence of flooding attacks in AODV.

IV. RESULTS

We have performed number of simulations to show the effectiveness, usefulness and performance of routing protocols architecture. We have run number of simulations with variable nodes and communication flows in each simulation; a node may have send data to other node or act as an intermediate node. Throughput and Packet delivery ratio and Normalized Routing Overhead is considered to evaluate the performance of the protocols.

A. Average Throughput

The figure 1 show the throughput of SAODV (green line) and normal AODV (red line) in manhattans grid and random waypoint mobility model respectively. After several numbers of simulations we find out the average throughput for both the protocols while randomly changing the values of node density. In SAODV average throughput decreases from 558 to 478 when node number increases 0 to 10 after that average throughput increases from 478 to 483 when node number increases from 10 to 20, after then average throughput decreases from 483 to 453 when node number increases from 20 to 30 on the other hand average throughput decrease linearly with respect to increase the node number from 0 to 30.

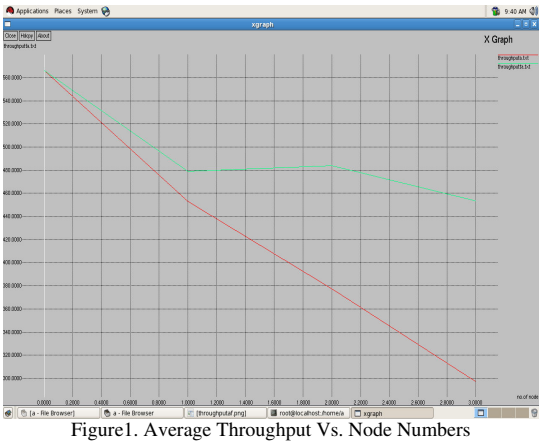

Figure1. Average Throughput Vs. Node Numbers

B. Packet Delivery Ratio

The figure 2 shows the packet delivery ratio of SAODV (green line) and normal AODV (red line) in manhattans grid and random waypoint mobility model respectively.

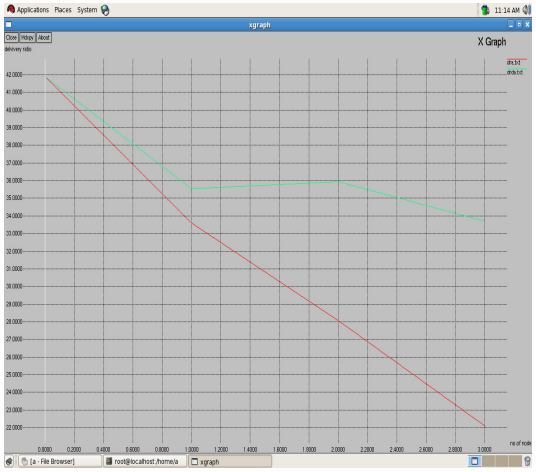

Figure 2: Packet Delivery Ratio Vs. Node Numbers

In SAODV packet delivery ratio decreases from 41.9 to 35.5 when node number increases 0 to 10 after that packet delivery ratio increases from 35.5 to 35.9 when node number increases from 10 to 20, after then average packet delivery ratio decrease from 35.9 to 34.8 when node number increases from 20 to 30 on the other hand packet delivery ratio decrease linearly with respect to increase the node number from 0 to 30.

C. Normalized Routing Overhead

The normalized routing overhead of SAODV and normal AODV in manhattans grid and random waypoint mobility model respectively. We run the simulations with constant traffic. We have the routing packets overhead with respect to number of nodes. SAODV routing overhead have increases for both mobility models as the number of nodes increases and AODV routing overhead change as number of nodes increases throughout simulation time. SAODV routing overhead mainly due to the lot of routing message generated by frequently after route failure.

V. CONCLUSION AND FUTURE WORK

In this paper, we evaluated secure (AODV) routing protocols for the mobile Ad-Hoc networks (MANETs) with the performance metrics despite the security metrics. The routing protocol SAODV takes advantage in term of end-to-end delay and packet delivery fraction over the normal AODV. As we have seen in the graphs the performance has increasing as the number of nodes is increased. The protocol overhead of SAODV is greater as compared to normal AODV. In the implementation of such routing protocols, the need is to eliminate the shortcoming of these protocols by evaluating performance of them on a simulation platform. To minimize the associated overhead like delay, routing overhead demands an intensive optimization in both the protocols. In future, more specifically SAODV is required to decrease the processing requirements to tackle hash chains and digital signatures to implement the security.

VI. REFERENCES

[1] Cuirong Wang, Shuxin Cai and Rui Li, "AODVsec: A Multipath Routing Protocol in Ad-Hoc Networks for Improving Security", IEEE 2009 International Conference on Multimedia Information Networking and Security, pp 401-404.

[2] Revathi Venkataraman, M. Pushpalatha, Rishav Khemka and T. Rama Rao, "Prevention of Flooding Attacks in Mobile Ad Hoc Networks", International Conference on Advances in Computing, Communication and Control (ICAC3'09), pp 525-529.

[3] Jun Pan and Jianhua Li, "MASR: An Efficient Strong Anonymous Routing Protocol for Mobile Ad Hoc Networks", IEEE 2009.

[4] L. Hanzo (II.) and R. Tafazolli, "Quality of Service Routing and Admission Control for Mobile Ad-hoc Networks with a Contention-based MAC Layer", IEEE 2006, pp 501-504.

[5] Wenchao Huang, Yan Xiong, Depin Chen, "DAAODV: A Secure Ad-hoc Routing Protocol based on Direct Anonymous Attestation", IEEE 2009 International Conference on Computational Science and Engineering, pp 809-816.

[6] A.H Azni, Azreen Azman, Madihah Mohd Saudi, AH Fauzi, DNF Awang Iskandar, "Analysis of Packets Abnormalities in Wireless Sensor Network", IEEE 2009 Fifth International Conference on MEMS NANO, and Smart Systems, pp 259-264.

[7] A Nagaraju and B.Eswar, "Performance of Dominating Sets in AODV Routing protocol for MANETs", IEEE 2009 First International Conference on Networks & Communications, pp 166-170.

[8] Sheng Cao and Yong Chen, "AN Intelligent MANet Routing Method MEC", 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp 831-834.

[9] WANG Xiao-bo ,YANG Yu-liang, AN Jian-wei, "Multi-Metric Routing Decisions in VANET", 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, pp 551-556.

[10] Dr Chandra Shekar Reddy Putta,Dr K.Bhanu Prasad ,Dilli Ravilla, "Performance of Ad hoc Network Routing Protocols in IEEE 802.11", IEEE 2010 International Conf. on Computer & Communication Technology, pp 371-376.