International Journal of Computer Applications Technology and Research
Volume 4– Issue 4, 327 - 330, 2015, ISSN:- 2319–8656

Preventing Disclosure Attacks by Secured Traffic Aware Protocol in Manets

S.Brindha Devi
Department of CSE
Panimalar Institute of Technology
Chennai,India

A. Porselvi
Department of CSE
Panimalar Institute of Technology
Chennai,India

Abstract: In this paper we propose a system that allows a safe and secure data transfer in MANETs between the source and the destination. As MANETs are unplanned networks and networks of instant communication, they are prone to attacks like disclosure, brute force attacks etc. In this paper we mainly concentrate on limiting the disclosure attacks in MANETs. Disclosure attack means that the network is monitored quietly without modifying it. The monitoring of network is possible only if the traffic is known. Hiding of traffic between the source and destination would prevent disclosure attacks in MANETs. To hide the traffic between the source and destination we must identify it. The traffic is identified using STARS(Statistical Traffic Pattern Discovery System for MANETs) technique. Using this technique, the traffic is made observable only for the intermediary nodes and the data is sent via intermediary nodes to the destination as single hop. The data which is sent as single hop by hop via intermediary nodes prevents the malicious node from knowing the original source and destination and thus preventing MANETs from disclosure attack.

1. INTRODUCTION

As networking is becoming an increasingly important technology for both military and commercial applications, security is an essential
requirement. MANETs are one of the network which is been widely used in the military environments. MANETs are used to start a instant communication between a source and the destination. MANETs are vulnerable to security attacks due to the lack of trusted authority and limited resources.

In mobile wireless networks there is no infrastructure, so it becomes even more difficult to efficiently detect the malicious activities that takes place inside the network. Because of this it becomes easy for the malicious nodes to flood the network withjunk packets or reveal the information by monitoring the network.

MANETs are usually prone to routing attacks because of their dynamic topology and less infrastructure .Attacks on network is of two categories

1.Active attacks.

2.Passive attacks.Active attacks are those which disrupt the normal functionality of MANETs such as doing data interruption, modification etc. Example: DoS, jamming. Passive attacks are those that do not disturb the functionality of MANETs but obtains the data that has been exchanged in the network. Example: traffic analysis, monitoring.Here, we majorly deals with passive attacks on MANETs such as traffic analysis and disclosure attacks. Traffic analysis in the MANETs are nothing but identifying the communication parties between whom and whom the communication is taking place and also finding their functionalities. This attacks takes place on data link layer of the network. This attacks can be prevented by encryption. But still nodes should continuously monitor time to time and look up for the malicious nodes to prevent from their misbehavior.

The goal of this paper is to prevent disclosure attacks in MANETs. Here in this attack, the malicious nodes
which is present as legitimate nodes in a network leaks confidential information to unauthorized nodes in the network. The best way to overcome this attack is by secure data transmission. For this secure data transmission, we use AOMDV protocol. This protocol discovers multiple path in a single route discovery and also uses hop- by- hop routing approach which hides the information about the actual source and the destination.

2. RELATED WORK

As the network evolves and the components in the network becomes bigger and bigger, network security becomes one of the important factor to be considered .By increasing the network security we can decrease the chance of piracy, spoofing , information theft etc.

In paper [1] proposed by David L.Chaun, they used a public key cryptography technique to hide the participant who is communicating with whom in a e- mail system.

In paper [2], Michael K.Reiter and Aviel D.Rubin introduced a system called CROWDS, where the users are grouped together to form a large group so that the web servers are unable to learn the true source of request.

In paper [3] Michael G.Reed, Paul F.Syverson proposed onion routing technique where data are encapsulated as layers to provide secure communication over public network.

In paper [4] Azzedine Boukreche, Khalil El-khalib, Lary Korba proposed a distributed routing protocol which makes sure that only the trustworthy intermediary nodes participate in the communication between source and the destination. In paper [5], Ronggong song, Lary korba, George Yee proposed a anonymous dynamic source routing
(AnonDSR) to provide user security.

In paper [6] Yanchao Zhang,Wei Liu proposed a anonymous

on- demand routing protocol termed as MASK which can accomplish MAC layer and Network layer communication without disclosing the real ID's.

In paper [7] S.Seys and B.Preneel proposed ARM(Anonymous Routing protocol) for MANETs that hides the routes.

In paper [8] Jiejun Kong, Xiaoyan Hong and Mario Gerla proposed two techniques namely identity-free routing and On - demand routing.

In paper [9] Reza Shokri, Maysam Yabandeh, Nasar Yazdani proposed a AODV protocol to provide sender and recipient relationship with least computational overhead.

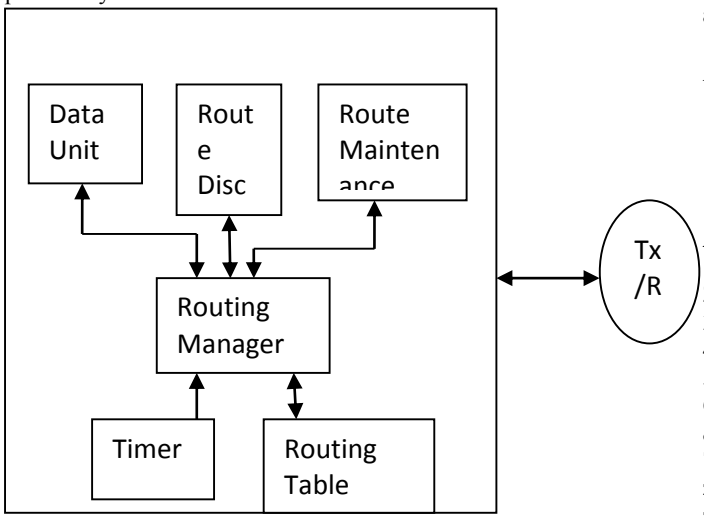
In paper [10] Xinyuan Wang, Shiping Chen and SushilJajodia proposed a water marking technique to identify the long flow between the original packet and anonymized waterflow.

3. PROPOSED WORK

To disclose the hidden traffic pattern in mobile networks, Statistical Traffic pattern discovery system (STARS) is used. STARS uses two major steps.

1.Point-to-point matrix to derive End-to-End matrix.

2. Analysing the end-to-end matrix to calculate the probability of each node to be a source or destination.



ROUTE DISCOVERY AND ROUTE MAINTAINENCE

In the intermediate node ,after receiving RREQ a reverse entry is set up by the node and it consists of all the details of it.when it reaches the destination and if both the IP address and the conditions are met then the RREQ gets response from the node to the source by means of unicasting RERR(route maintenance) is initiated by the node upstream (closer to the source) of the break, Its propagated to all the affected destinations. RERR lists all the nodes affected by the link failure Nodes that were using the link to route messages (precursor nodes). When a node receives an RERR, it marks itsroute to the destination as invalid Setting distance to the destination as infinity in the route table.When a source node receives an RRER, it can reinitiate the route discovery.

POINT-TO-POINT MATRIX:

With the captured point-to-point traffic(one hop) in a certain period T, we build up point-to-point traffic matrices. We construct this point to point matrices such that each traffic matrix contain only independent one hop packets. To avoid a single point-to-point traffic matrix from containing two dependent packets, we apply slicing technique. That is we take snapshots of the network and each snapshot is triggered by a captured packet. A sequence of snapshots during a time interval (Δtc) construct a slice represented by traffic matrix which is N*N one hop matrix. When calculating length of the time interval we consider two important criteria.

1. In the time interval node can either be sender or receiver.
2. Each matrix must represent one hop transmission during the time interval.

The time slicing technique which is done here is to make sure that packets captured in time interval are independent of each other. Each packet p in Wc(i,j) has three features P.vsize,P.time and P.hop. A packet hop count is set to 1.

W1=[0 1 0,0 0 0,0 0 0]

END-TO-END MATRIX:

From the given sequence of point-to-point matrix we derive end-to-end matrix R=(r(i,j)) N*N where r(i,j) is the accumulative traffic volume from node i to node j.

Algorithm 1. —f(W| 1*K).
1: R = W1
2: for e = 1 to K-1 do
3: R = g(R;We+1) + We+1
4: end for
5: return R

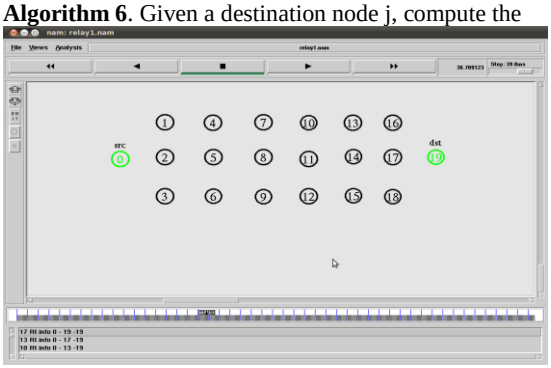
Algorithm 2. —g(R,We+1)
1: R'= R
2: for i = 1 to N do
3: for k = 1 to N and k ≠ i do
4: for j =1 to N do
5: for each x € we+1(j, k).pkt do
6: if y € r(i, j).pkt s.t. x.time – y.time < T and y.hop < H then
7: create z with z.time =x.time
z.hop =y.hop + 1
z.vsize = min{x:vsize, y:vsize}
8: r'(i, k).pkt = r'(i; k).pkt U {z}
9: r'i; k) = r'i, k) + z.vsize
10: end if
11: end for
12: end for
13: end for
14: end for
15: return R'

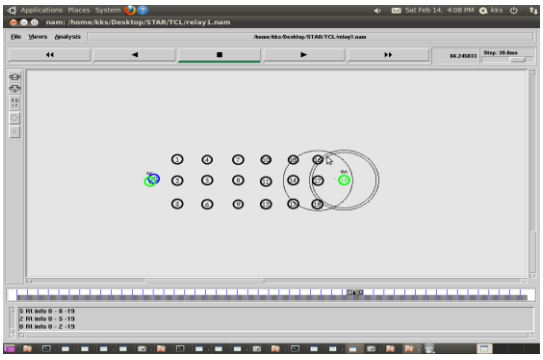
Algorithm 3. —Src(R).
1: S0 = (1/N, 1/N, . . . , 1/N)
2: n = 0
3: do
4: Sn+1 = (¢(R) . ¢ T(R)) . Sn
5: normalize Sn+1
6: n =n + 1
7: while Sn ≠Sn-1
8: S =Sn
9: return S

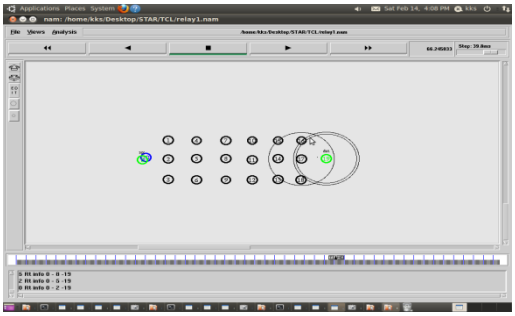
Algorithm 4. —Dest(R) .

1: D0 =(1/N, 1/N; . . . , 1/N)
2: n = 0
3: do
4: Dn+1 = (¢T(R). ¢ (R). Dn
5: normalize Dn+1
6: n = n + 1
7: while Dn ≠ Dn-1
8: D = Dn
9: return D
Algorithm 5.

Given a source node i, compute the
probability distribution vector Ls-d(i) for each node
to be the intended destination of i.
1: R = f(W|1 *K);
2: D = Dest(R);
3: W '|1*K = Suppress-Sender(i);
4: R0 = f(W '|1*K);
5: D-= Dest(R');
6: Calculate the probability reduction vector as:
L's-d(1)= D -D-. If negative elements exist in L's-d (1)
increase each element by the absolute value of the
smallest negative element;
7: Normalize L's-d (1) to generate the probability vector
L's-d (1) for each node to be the intended destination of i;
8: Return L's-d (1)
Algorithm 6. Given a destination node j, compute the







probability distribution vector Ld-s (j)for each node to be the corresponding source of j.
1: R =f(W|1*K);
2: S = Src(R);
3: W'|1*K = Suppress -Receiver(j);
4: R0 = fõW '|1 *K);
5: S- = Src(R ');
6: Calculate the probability reduction vector as:
L'd-s (j)S – S-. If negative elements exist in L'd-s (j)increase each element by the absolute value of the
smallest negative element;
7: Normalize L'd-s (j) to generate the probability vectorLd-s (j) for each node to be the corresponding source of j;
8: Return Ld-s (j)
Once we find the hidden traffic pattern between the source and destination using STARS we hide the traffic from the malicious nodes. This is done by making the nodes in the network observable or visible only for trustworthy nodes. The data is send from source to destination in a hop by hop manner. That is the information about the actual source and destination is hidden in the routing table. The routing table consists of source and the next intermediary node as destination. After one hop the destination node becomes the source and the next intermediary node in the path that reaches the final destination become the next destination. In this manner the data sent reaches the final destination. Even if the malicious nodes are present in the actual traffic, it cannot track or disclose the traffic to the unauthorized nodes which in turn leads hacking of the data.

4. CONCLUSION

Here we use STARS which is generally an attacking system that discloses the traffic pattern to the malicious nodes. Using the above system we find the actual traffic and hide the traffic to the untrustable nodes. Thus, this helps in preventing disclosure attacks in MANET

5. REFERENCES

[1] D. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability," J. Cryptology, vol. 1, no. 1, pp. 65-75, 1988.
[2] M. Reiter and A. Rubin, "Crowds: Anonymity for Web Transactions," ACM Trans. Information and System Security, vol. 1, no. 1,pp. 66-92, 1998.
[3] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous Connec- tions and Onion Routing," IEEE J. Selected Areas in Comm., vol. 16, no. 4, pp. 482-494, May 2002.
[4] A. Boukerche, K. El-Khatib, L. Xu, and L. Korba, "SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks," Proc. IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN '04), pp. 618-624,2004.
[5] R. Song, L. Korba, and G. Yee, "AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks," Proc. Third ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '05), pp. 33-42, 2005.
[6] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "MASK: Anonymous On- Demand Routing in Mobile Ad Hoc Networks," IEEE Trans. Wireless Comm., vol. 5, no. 9, pp. 2376-2385, Sept. 2006.
[7] S. Seys and B. Preneel , "ARM: Anonymous Routing Protocol for Mobile Ad Hoc Networks,"
Proc. IEEE 20th Int'l Conf. Advanced Information Networking

and Applications Workshops
(AINA Work- shops ’06), pp. 133-137, 2006.
[8] J. Kong, X. Hong, and M. Gerla, “An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks,” IEEE Trans. Mobile Computing, vol. 6, no. 8, pp. 888-902, Aug. 2007.
[9] R. Shokri, M. Yabandeh, and N. Yazdani, “Anonymous Routing in MANET Using Random Identifiers,” Proc. Sixth