A SYMMETRIC TOKEN ROUTING FOR SECURED COMMUNICATION OF MANET

J. Thangakumar and M. Roberts Masillamani

School of Computer Science & Engineering, Hindustan University, Chennai, India

thang.kumar@gmail.com & deancs@hindustanuniv.ac.in

Abstract: The communication should be much secured in Mobile Adhoc Networks in the protective environment such as Military atmosphere and in a disaster relief. Due to the attackers, Mobile Adhoc Networks resulting in denial of Service attacks modify packets, Error packets, Missing Packets, Theft of Nodes, etc. To overcome this problem, We propose a new Symmetric Token Routing Protocol (STRP) for mobile ad hoc networks provides much security against MANET. The proposed protocol distributed a secured shared symmetric token for each node to provide security against hackers and attackers. Simulation results shows the better delivery against the existing protocol in MANET.

Keywords: MANETs, Symmetric Token Routing Protocol, Hop Count.

1. INTRODUCTION

A mobile ad hoc network (MANET), sometimes called a mobile mesh network, is a self-configuring network of mobile devices connected by wireless links. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic [2]. Such networks may operate by themselves or may be connected to the larger Internet.

Authentication research has determined that for a positive identification, elements from at least two, and preferably all three, factors [3, 4, 5] be verified. The three factors (classes) and some of elements of each factor are:

1. The ownership factors: Something the user has (e.g., wrist band, ID card, security token, software token, phone, or cell phone)
2. The knowledge factors: Something the user knows (e.g., a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question))
3. The inherence factors: Something the user is or does (e.g., fingerprint, retinal pattern, DNA sequence (there are assorted definitions of what is sufficient), signature[6,7], face, voice, unique bio-electric signals, or other biometric identifier).

Nabendu Chaki et al. (Eds.): NeTCoM 2010,CSCP 01, pp. 17–24, 2011.
 DOI : 10.5121/csit.2011.1102

1.1 CHALLENGES IN MANET

In order to provide protected communication between mobile nodes in a hostile environment security has become a primary concern [1]. In contrast to the wire line networks, a number of nontrivial challenges are posed to security design by the unique characteristics of mobile ad hoc networks, for instance open peer-to-peer network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. The research activities about security in MANETs are still at their beginning, while the routing aspects of MANETs are already well understood. In addition to the problems of regular networks, a number of new security problems are also faced by MANETs [2].some of the vulnerabilities are as follows.

MANET nodes would not be any safe. The node could be compromised and thus would act as a hostile node. Easy theft might also lead to node tampering. Tampered node might disrupt network operations or release critical information. Securing such a protocol in the presence of hostile nodes presents a challenge.

Without appropriate protection, the malicious nodes can readily function as routers and prevent the network from correctly delivering the packets. For example, the malicious nodes[8] can announce incorrect routing updates which are then propagated in the network, or drop all the packets passing through them. Thus security issue in ad hoc networks, namely the protection of their network-layer operations from malicious attacks is very important.

1.2 NEEDS OF MANETS

All Secure ad hoc routing protocols must satisfy the following requirements to ensure that path discovery from source to destination functions correctly in the presence of malicious adversaries [7].

The network topology must not be exposed neither to adversaries nor to authorized nodes by the routing messages. Exposure of the network Topology may be an advantage for adversaries trying to destroy or capture nodes.

Significant work focused on the security of uni-cast wireless routing protocols. Several secure routing protocols resilient to outside attacks such as authentication were proposed in the last few years such as Ariadne [3], SEAD [8], and ARAN [7]. Several routing protocols were proposed to cope with insider attacks such as dropping packets, modifying packets [3] – [6]. Methods proposed to address insider threats in routing include monitoring [4], multi-path routing [3], [5] and acknowledgment-based feedback [5].

1.3 ATTACKS

Not forwarding packets, injecting, modifying or replaying packets, rushing packets or creating wormholes are some examples of such behaviour.

1. An attack can drop the request and/or response, or can influence the route selection by using wireless specific attacks such as wormhole and flood rushing to prevent a route from being established.
2. In addition, the packets carrying the route selection metric such as hop count or node identifiers can be modified by the attacks.
3. Termination of routes due to unpredicted movement of the node in the network can drop the request or response [11].

We propose a new Symmetric Token Routing Protocol (STRP) that provides resilience against such attacks to mitigate these vulnerabilities of routing protocols in wireless ad hoc networks.

2 RELATED WORKS

Attacks against routing in ad hoc networks were presented by YihChun H. In addition, the design of Ariadne, a new secure reactive adhoc network routing protocol was presented and its performance was evaluated. In addition, it prevents a large number of types of Denial-of-Service attacks [3].

Two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so are presented by Sergio Marti. They have proposed categorizing nodes based upon their dynamically measure behaviour to mitigate this problem. [4].

The SMT and SSP protocols for secure data communication in ad hoc networks were presented and analyzed by Panagiotis Papadimitratos and Zygmunt J. Haas. Owing to the fact that the two protocols provide lightweight end-to-end security services and operate without knowledge of the trustworthiness of individual network nodes, they are applied extensively [5].

An routing protocol for ad hoc wireless networks that provides resilience to failures caused by individual or colluding nodes was presented by Baruch Awerbuchl. After log n faults have occurred (where n is the length of the path), a malicious link is detected by their adaptive probing technique. [6].

The notion of a tunneling attack, in which collaborating malicious nodes can encapsulate messages between them to subvert routing metrics, was introduced by Kimaya Sanzgiri, et al. A solution for secured routing in the managed-open environment was provided by their protocol [7].

The design and evaluation of SEAD, a secure ad hoc network routing protocol using distance vector routing was presented by Yih-Chun Hu, et. al. They used efficient one-way hash functions against Denial-of-Service (DoS) [8].

Gergely Acs [9] have argued that flaws in ad hoc routing protocols can be very subtle, and they advocated a more systematic way of analysis. They have proposed a mathematical framework in which security can be precisely defined and routing protocols for mobile ad hoc networks can be proved to be secure in a rigorous manner.

Syed Rehan Afzal et al. [10] have explored the security problems and attacks in existing routing protocols and then they have presented the design and analysis of secure routing protocol, called SRP. The proposed (SRP) secure routing protocol was based on DSR, which uses a broadcast authentication scheme.

3 AODV PROTOCOL PROBLEM

The AODV [17, 18] routing protocol is a reactive routing Protocol; therefore, routes are determined only when needed. The message exchanges of the AODV protocol is given below.

Hello messages may be used to detect and monitor links to neighbours. If Hello messages are used, each active node Periodically broadcasts a Hello message that all its neighbours receive.

Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbour, a link break is detected.

When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is uni-cast in a hop-by hop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. When the source receives the RREP, it records the route to the destination and can begin sending data. If multiple RREPs are received by the source, the route with the shortest hop count is chosen.

As data flows from the source to the destination, each node along the route updates the timers associated with the routes to the source and destination, maintaining the routes in the routing table. If a route is not used for some period of time, a node cannot be sure whether the route is still valid; consequently, the node removes the route from its routing table.

If data is flowing and a link break is detected, a Route Error (RERR) is sent to the source of the data in a hop-by hop fashion. As the RERR propagates towards the source, each intermediate node invalidates routes to any unreachable destinations. When the source of the data receives the RERR, it invalidates the route and reinitiates route discovery if necessary. This process will be repeated again and again.

4 SYMMETRIC TOKEN ROUTING PROTOCOL (STRP)

4.1 SHARED KEY TECHNIQUE

We employ an authentication framework which eradicates a large class of outside attacks by ensuring that only authorized nodes can perform certain operations. Every node authorized to take part in the routing and data transmission is presented with a pair of public/private keys and a node certificate that connects public key of the node to its IP address. The token used to authenticate the nodes to be communicated in the network is periodically refreshed and disseminated by a special node, authorizer. Consequently, only the nodes that are currently participating in the routing or data forwarding operations will possess a valid tree token.

Both route request and route reply are flooded by the protocol which guarantees that a path is established even if route activation messages are dropped to mitigate inside attacks that try to prevent a node from establishing a route to the destination by employing a timeout based mechanism. If an adversarial-free route subsists, the protocol ensures the reaction of a route.

In order to provide resilience to selective data forwarding attacks, a reliability metric containing a list of link weights where high weights correspond to low reliability to capture adversarial behaviour, is employed. Every node maintains its own weight list and includes it in each route request to ensure that a new route to the tree avoids adversarial links. The link's reliability is determined by the number of packets successfully delivered on that link. The destination node monitors the rate of receiving data packets and it is compared with the transmission rate specified by the source. If the variation amid the perceived transmission rate and the rate specified by the source on a link falls below a threshold value, the weight of that link is enhanced. Subsequently, the discovery of a new route is initiated.

4.1.1 SYMMETRIC TOKEN DISTRIBUTION

We consider a multi- hop wireless network where nodes participate in the data forwarding process for other nodes. We assume that the wireless channel is symmetric. All nodes have the same transmitting power and consequently the same transmission range. The receiving range of a node is identical to its transmission range. Also, nodes are not required to be tamper resistant: If an attacker compromises a node, it can extract all key material, data or code stored on that node.

We assume that nodes have a method to determine the source authenticity of the received data. The framework prevents unauthorized nodes to be part of the network or of the routing path. Each authorized node of the network has a pair of public/private keys and a node certificate that binds its public key to its IP address.

4.1.2 CIRCULATION BETWEEN NODES

The source node employs the pair-wise shared keys established between the neighbors to periodically refresh and broadcast the token used to authenticate all the nodes along the routing path. Hence, a valid token will be possessed by the nodes that are at present on the routing path. The source utilizes a one-way hash function F to periodically broadcast a token authenticator in the whole network. Nodes can apply the function F to the route token and compare it with the last received token authenticator to authenticate it.

4.1.3 HOP COUNT

The source node S calculates the hop count index

$$HI=f^{dm}(X)$$

Where X is a random number selected by S. A node[6] along the routing path receives the following information from its parent:

$$[X, d, dm, f^{dm}(X)]$$

Where d is the parent's hop distance to the source and $f^{dm}(x)$ is the hop count index.

4.3 ROUTE DISCOVERY

A modified route request/route reply procedure utilized by the reactive routing protocols is employed by the protocol. The route request (RREQ) message created by the source node and signed using its private key includes the node id, its weight list, and a request sequence number in a concatenated format.

Only if the total weight is less than any previously forwarded RREP message with same response sequence number, the hop count authentication and all the signatures collected on the response are considered to be valid. After the validation of the message, the node adds its id to the message and updates the hop count authentication information. Subsequently, the node signs the entire message and rebroadcasts it. While the RREP message propagates across the network, the nodes set pointers to the node from which the RREP was received in order to establish the forward route.

The procedure followed by the intermediate nodes during the RREP propagation when it receives a RREP is also performed by the source. Besides, the source verifies the validity of the route token included in the RREP message.

The source periodically broadcasts the data transmission rate R in a message (TR_MSG) after signing it. Nodes which receive this message, add their estimated transmission rate to the message and stores the copy of the last received TR_MSG.

5 SIMULATION

We use NS2 to simulate our proposed algorithm. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps.

Table 1. Parameter for our Simulation

No. of Nodes	25
Area Size	500 X 500
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 KB/s
Speed	5m/s t 10m/s
Misbehaving Nodes	5,10,15 and 20

6 RESULTS

Average Packet Delivery Ratio: This is the fraction of the data packets generated by the sources that are delivered to the destination. This evaluates the ability of the protocol to discover routes [7]

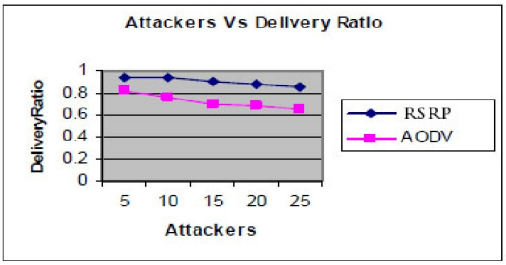

Figure. 1. Attackers Vs Delivery Ratio for 25 Nodes

Fig. 1 shows the results of delivery ratio for the misbehaving nodes 5,10,….to 25 nodes scenario. Clearly our STRP scheme achieves more delivery ratio than the AODV scheme since it has better reliability compared with AODV.

7 CONCLUSION

We proposed a new Symmetric Token Routing Protocol (STRP) that provides resilience against such all attacks. Since existing routing protocols provide solutions separately for insider attacks, outsider attacks and selective forwarding attacks, our proposed protocol provides total

protection against all these attacks. Through simulation results, we have demonstrated that STRP effectively mitigates the identified attacks with stronger resistance against node capture by providing better delivery ratio.

REFERENCES

[1]. Zhang, L.: Security in mobile ad hoc networks: Challenges and solutions. IEEE Proceedings on Wireless Communications 11(1), 38–47 (2004), doi:10.1109/MWC.2004.1269716

[2]. J.Thangakumar & Dr. Roberts Masillamani, An Enhanced Secured Communication Of MANET Springer Series on Advances in Networks & Communication, CCSIT 132, Part II, PP 340 -348, January 2011

[3]. Hu, Y., Perrig, A., Johnson, D.B.: Ariadne: A Secure ReactiveRouting Protocol for Ad Hoc Networks. In: Wireless Networks (WINET), vol. 11(1-2), pp. 21–38. ACM, Springer (January 2005)

[4]. Marti, S., Giuli, T.J., Lai, K., Baker, M.: Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. In: Proc. of 6th Annual International Conference on Mobile Computing and Networking, pp. 255–265 (2000)

[5]. Papadimitratos, P., Haas, Z.J.: Secure Data Communication in Mobile Ad Hoc Networks. Proceedings of IEEE Journal on Selected Areas in Communications 24(2) (February 2006)

[6]. Awerbuch, B., Holmer, D., NitaRotaru, C., Rubens, H.: An On Demand Secure Routing Protocol Resilient to Byzantine Failures. In: Proc. of 1st ACM Workshop on Wireless Security, pp. 21–30 (2002)

[7]. Sanzgiri, K., Dahill, B., Levine, B.N., Shields, C., Belding-Royer, E.M.: A Secure Routing Protocol for Ad Hoc Networks. In: Proc. of 10th International Conference on Network Protocols, November 12-15, pp. 78–87 (2002)

[8]. Hu, Y.-C., Johnson, D.B., Perrig, A.: SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks. In: Proc. of 4th IEEE Workshop on Mobile Computing Systems and Applications, pp. 3–13 (2002), doi:10.1109/MCSA.2002.1017480

[9]. Acs, G., Buttyan, L., Vajda, I.: Provably Secure ReactiveSource Routingin Mobile Ad Hoc Networks. IEEE Transactions on Mobile Computing 5(11) (November 2006)

[10]. Afz al, S.R., Biswas, S., Koh, J.-b., Raza, T., Lee, G., Kim, D.-k.: RSRP: A Robust Secure Routing Protocol for Mobile Ad hoc Networks. In: Proc. of IEEE Conference on Wireless Communication and Networking, Las Vegas, NV, March 31- April 3, pp. 2313–2318 (2008), doi:10.1109/WCNC.2008.408

[11]. Masillamani, M.R., Jamalipour, A.: Intelligent MANET. Hindustan Journal 3, 73–80 (2010)

Authors

Dr. M Roberts Masillamani received his B.E. degree in Electrical and Electronics Engineering from RECT in 1974. He obtained his Masters from IIT Madras and Doctorate from the faculty of Information and Communication Engineering, Anna University, Chennai. He is an alumni of REC Trichy, IIT Madras, Anna University, SRM University, University of Sydney, and Haggai Institute USA. Dr. Roberts has 36 years of Industrial, Administration, Academic and Research experience. He has to his credit quite a few papers in refereed International journals and Conferences. He is member of ISTE, IE, ITEEA, AACE, CSI and IEEE as well. He is now the Dean, Computing Sciences at the Hindustan Institute of Technology & Science, Chennai, Tamilnadu, India.

J. Thangakumar received his B.E Degree in Electrical & Electronics Engineering from Dr.Sivanthi Aditanar College of Engineering, Tamilnadu in 2003, He obtained his M.tech in Computer Science & Engineering, SRM University, Chennai. He is presently working as Assistant professor in Hindustan Institute of Technology & Science, Chennai, Tamilnadu, India. He has six years of industrial, academic and research Experience. He is a Member of IEEE & CSI. His area of Interests is Mobile Ad hoc Networks, Cryptography & Network Security, Data mining & software Engineering.