Journal of Computer Science 7 (5): 651-656, 2011
ISSN 1549-3636

Authentication Based and Optimized Routing Technique in Mobile Ad hoc Networks

S. Varadhaganapathy, A.M. Natarajan and S.N. Sivanandam
Department of IT, Kongu Engineering College, Perundurai-638 052, Tamilnadu, India
Department of ECE, Bannari Amman Institute of Technology, Sathyamangalam,
Dean/Advisor, Sri Akshaya College of Engineering and Technology, Coimbatore, Tamilnadu, India

Abstract: Problem statement: An Ad hoc network has been defined as a self-organizing, dynamic topology network formed by a group of wireless mobile nodes. Minimal configuration, absence of infrastructure and quick deployment, would make ad hoc networks convenient for emergency situations other than military applications. In recent years, security in Ad hoc Networks as a research topic had started to receive attention from a growing number of researchers. **Approach:** Several ad hoc network routing protocols have been proposed; only some of them consider the security problems. To secure an ad hoc network, the attributes like availability, confidentiality, integrity, authentication and non-repudiation may be considered. In this study, authentication is taken into consideration. Here, Double Hash Authentication Technique (DHT) has been incorporated for ad hoc networks. The security associations between nodes were established, when they were in the vicinity of each other, by exchanging appropriate cryptographic information. This security mechanism has been simulated on Dynamic Source Routing (DSR) protocol in addition to Self-Healing and Optimized Routing Technique (SHORT) made the routing secure for ad hoc networks. **Result:** The results have shown that in a moderately changing network, the Double Hash Technique has provided secure routing even in the presence of malicious nodes. **Conclusion:** The Double Hash Technique in association with SHORT has improved the performance of the DSR protocol.

Key words: Double Hash Authentication Technique (DHT), ad hoc network, Dynamic Source Routing (DSR), SHORT, Source Address (SA), Destination Address (DA), Neighbor Node Address (NA), malicious node, routing protocols, network topology

INTRODUCTION

Ad hoc networks are a new paradigm of wireless communication for mobile hosts (which we call nodes). In an ad hoc network, there is no fixed infrastructure such as base stations (Zabian *et al*., 2008) or mobile switching centers. Mobile nodes within each other's radio range communicate directly via wireless links, while those that are far apart rely on other nodes to relay messages as routers. Node mobility in an ad hoc network causes frequent changes of network topology (Khatri *et al*., 2010).

Security (Hao *et al*., 2004) in MANET is an essential component for basic network functions like packet forwarding and routing. Wireless networking is an emerging technology that allows users to access information and services electronically, regardless of their geographical position. Previous works proposed the idea of incorporating the security attributes as parameters into ad hoc route discovery and protecting the multi-hop network connectivity between nodes in a MANET. In this study, the secured routing between the nodes is incorporated.

MATERIALS AND METHODS

DSR routing protocol: The Dynamic Source Routing (DSR) (Khatri *et al*., 2010) protocol is a simple efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain source routes to arbitrary destinations in the ad hoc network.

Securing DSR: Mobile networks are generally more prone to physical security threats (Isaac *et al*., 2010; Yampolskiy and Govindaraju, 2007) than fixed cable networks. As a result of this physical security, the nodes can misbehave and can change its characteristics. These nodes are called malicious or compromised nods. A malicious node (compromised node) can perform

Corresponding Author: S. Varadhaganapathy, Department of IT, Kongu Engineering College, Perundurai-638 052 Tamilnadu, India Tel: 04294-226570 Fax: 04294-220087

many kinds of attack just by not following the DSR rules (Liu *et al*., 2007). Assuming that the malicious node is M, the originator is S and the destination node is D, the malicious node M can carry out several attacks against DSR protocol (Koul *et al*., 2008).

A secure key management sub-system that makes it possible for each ad hoc node to obtain public keys of the other nodes of the network is assumed for instance. Two mechanisms are used to secure the DSR messages. The first one uses the digital signature (Safdar *et al*., 2006) to authenticate the non-mutable fields of the messages and the second one uses the hash chains to secure the only mutable information, the hop count. The information related to the digital signatures and the hash chains is then transmitted with the DSR messages as an extension message.

Security mechanisms: In recent years, security in Ad hoc Networks as a research topic has started to receive attention from a growing number of researchers. Several ad hoc network routing protocols (Vijayaragavan *et al*., 2009; Alfawaer *et al*., 2007a) have been proposed for routing as well as data, but none of them considers the security problems. On-demand routing protocols (Khatri *et al*., 2010) provide scalable and cost effective solutions for packet routing. The path generated by these protocols may deviate from the optimal path due to lack of knowledge about mobility and global topology of nodes. The routing (Alandzi and Quintero, 2007) optimality affects the network performance.

In this study, an efficient security mechanism based on Dynamic Source Routing (DSR) protocol has been put forward to improve the security in ad hoc networks. The DHT Authentications are adopted as the security mechanisms to protect the routing information (Sanzgiri *et al*., 2005).

Double hash authentication: The Fast and Efficient Hash function is adopted to authenticate routing information instead of digital signatures. Under the reasonable assumption that no two compromised nodes are colluding and are within two hops of each other. In this double Hash authentication one of which is used to authenticate the received routing packets and other is used to prevent the current nodes modifying the routing information themselves (Liu *et al*., 2007). If some compromised node modified the routing information, its neighboring nodes can detect the misbehavior immediately. In an initial phase each node makes use of the management of local node group to distribute the common secret with its two hop node group.

Distribution of common secret key: In this technique each node needs to distribute a common secret by its two-hop node group. This secret key is kept secret against its one-hop node group. Each node has a pair of private and public keys (widely known) (Zhang *et al*., 2010). The source node generates random key Ks and encrypts it with the public key of the nodes within two-hop. On receiving the encrypted key each node decrypts it with the corresponding private key and gets the common secret key Ks. Due to the mobility, ad hoc network can result in the change of the local node groups and the distribution of the common secrets should be adjusted timely. When some new nodes join in two hop node group, the source node needs to distribute Ks to those new nodes and if some nodes within two-hop becomes the member of its one-hop node group(due to roaming) the source needs refreshing and redistribution of Ks.

Double hash algorithm: The Public one way hash function H(.) is used to authenticate the RREQ twice, so the routing packets includes not only the RREQ but also two hash values(H1,H2), where H2 is used to check whether the received routing packet has been modified and H1 is used to prevent the current node modifying the packet. The algorithm (Jayakumar and Gopinath, 2007) is as follows:

- Generate RREQ from source node RREQ={S,L,H,R}
- S- Source Identity; L- sequence number (RREQ)
- R- Routing information. H- Hop count.
- Source multicasts{S, L+1, H, R, H1, 0} to its multicasts group
- Any intermediate node within this group can verify the authenticity of packet. H2=0(from source node); H1 = H(S\L+1\H\R\K) K- Secret key shared by two-hop node and source
- Before forwarding the packet increment the hop count by 1 and copy H1 to H2 and calculate the new H1. i.e. H1=H(S\L+1\H+1\R\Ki); H2=H(S\L+1\H\R\K) where Ki is common secret key between intermediate node and two hop node
- Forward the Routing packet to its Multicast group
- On Receiving {S\L+1\H+1\R\H1\H2} nodes within the group can use {S, L+1, H+1, R} and public hash function to calculate H(S\L+1\H\R\K)
- Compare this value with H2 and validate whether routing packet is modified by intermediate node
- If intermediate node wants to modify the packet it has to forge the H2 value before forwarding the packet

The same concept is applied for RREP from destination to source.

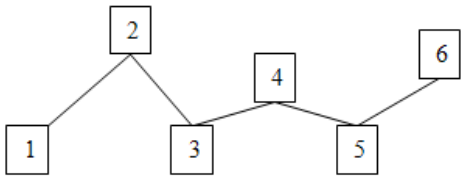

Fig. 1: Routing path

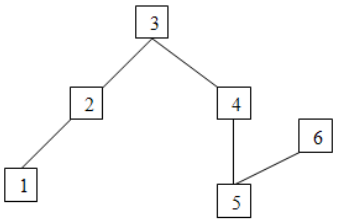

Fig. 2: Path change due to mobility

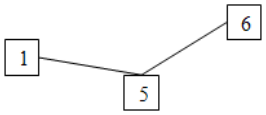

Fig. 3: Short-cut path

Self healing and optimizing routing technique (short): On demand routing protocols (Mallah and Quintero, 2009) provide scalable and cost-effective solutions for packet routing (Al-Bdour, 2005) in mobile wireless ad hoc networks. The paths generated by these protocols may deviate far from the optimal because of the lack of knowledge about the global topology and the mobility of nodes. Routing optimality affects network performance and energy consumption, especially when the load is high. This study, uses Self-Healing and Optimizing Routing Technique (Short) for mobile ad hoc networks. While using SHORT, all the neighboring nodes monitor the route and try to optimize it if and when a better local sub-path is available. Thus SHORT enhances performance in terms of bandwidth and latency without incurring any significant additional cost.

With the increase in the size and average route length (Bhalaji *et al*., 2008), scalability becomes an issue for the current ad hoc routing protocols. Table-driven pro-active routing protocols that require periodic advertisement and global dissemination of connectivity information are not suitable for large networks. On-demand routing protocols are efficient for routing in large ad hoc networks (Hanapi *et al*., 2009) because they maintain the routes that are currently needed, initiating a path discovery process whenever a route is needed for message transfer. AODV (Pirzada *et al*., 2006; Alfawaer *et al*., 2007b) and DSR (Pirzada *et al*., 2006; Koul *et al*., 2008) are two prominent ad hoc routing protocols that have used this approach. In DSR, the routing table at the nodes caches the next hop router information for a destination and use it as long as the next hop router remains active (originates or relays at least one packet for that destination within a specified time-out period). This SHORT technique is applied to Double Hash Technique to reduce the associated delay.

Features of short:

- It monitors the Route(Path)
- Shorten the path if shortcut is available
- Enhance the performance in terms of bandwidth without any additional cost

Basic concepts of short:

- Nodes transmit packet within its transmission range
- Receiving node checks header of the packet
- Each packet carries Hop count (HP), Source Address (SA), Destination Address (DA), Neighbor Node Address (NA)
- Information is stored in HOP comparison Array
- New entries replace the old entries when the array is full

In the Fig. 1 initial path is discovered from node 1 to node 6 by the route discovery process. Here packet takes 5 hops while getting routed from node 1-6. During the course of time the mobility of node changes hence, results in the change of shape as shown in Fig. 2. By using the SHORT algorithm it is possible to find the shortcut path from node 1-6 as shown in Fig. 3.

Short algorithm:

- Check whether the address is the final destination address, if true consume the packet else check whether packet is destined to next hop node if true process the packet further
- Check for an entry corresponding to<S, D> exists in the hop count array if doesn't, record the information :< S, D, H, N> else compare <S, D> to all valid entries in the hop comparison array. S-Source; D- Destination; H- Hop count; N-Neighbor node

- When there is no match with the entries store <S,D,H,N> in the hop comparison array else if C>2 then send a message to N1(node) to update the routing table such that the next hop address for destination node D is modified to the address of node 1. C- Comparison between two nodes
- The node 1 modifies its routing table by making the next hop address for destination D as N2(node)
- The entry corresponding to <S,D> is deleted from the hop comparison array maintained at node 1
- End of the algorithm

Disadvantages: This algorithm doesn't react to very little changes in the network topology.

Simulation environment
Simulation parameters:

- 300×300 m area
- Maximum 70 nodes, Random node placement
- Mobility model-Random Waypoint
- Radio model-Two Ray Ground set model
- Omi directional antenna
- Source agent-UDP, destination agent -Null
- Maximum velocity of nodes-10m/s, 20 m/s
- Bandwidth-2Mbps
- Constant Bit Rate traffic source
- Packet size-512, No of packets 100, packet interval 4.0
- Simulation time-100 seconds and 900 seconds
- MAC Protocol-802.11b

Analysis of DSR: Consider a group of 40 nodes. Consider node 26 is the source node that transmits the packets and node 3 is the destination node that receives the packets. First the source node broadcasts the RREQ packet to all the nodes. The intermediate nodes receive the RREQ from source node and broadcast the RREQ to find the destination node. After receiving the RREQ from node intermediate node the destination node replies with a RREP. So a path is setup between source node and destination via the intermediate nodes. When the path setup is completed, the data transmission begins. It is assumed that node 36 is a malicious node and hence it may or may not forward the data packets to the destination node. As a result, all the messages transmitted by node may or may not reach the destination node.

Analysis of DHT: Consider the same case as above for the analysis of Dual Hash Technique (DHT). The RREQ broadcast reaches the destination node from the source node in the same manner as above. But in this case, DHT prevents the packets entering the malicious node, as a result the packets transferred in alternate paths to destination.

RESULTS

Figure 4 shows packet Delivery Ratio (Murugan and Shanmugam, 2010; Peng and Deyun, 2006) of DSR, Dual Hash Technique and SHORT. The packets may travel through malicious node in DSR hence the delivery ratio of DHT is better than DSR and SHORT is still better. Here, SHORT provides a delivery ratio of 0.3 % more than DHT and 0.8% than DSR.

Figure 5 shows the Node Vs Control Overhead (Barati *et al*., 2008) for DSR, Dual Hash Technique. Here the control packets increase when the node increases. Dual Hash Technique has less control packets compared to DSR and SHORT has further reduced them. Control overhead has been reduced by 1.6% in DHT and 11.4% in SHORT when compared to DSR.

Figure 6 shows the Pause Time Vs Delivery Ratio for DSR (Patel and Goel, 2006), Dual Hash Technique and SHORT. When the pause time increases the node movement reduces from one place to other. Due to this the delivery ratio is increased. Dual Hash Technique has a delivery ratio of 0.4% more than DSR and SHORT has a delivery ratio of 0.065 % more than DHT.

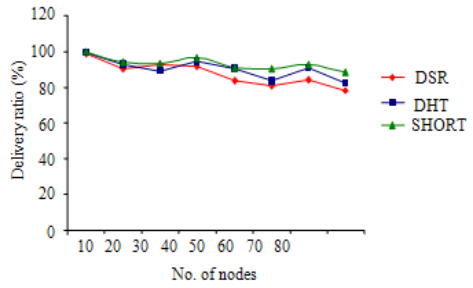

Fig. 4: No. of nodes and delivery ratio

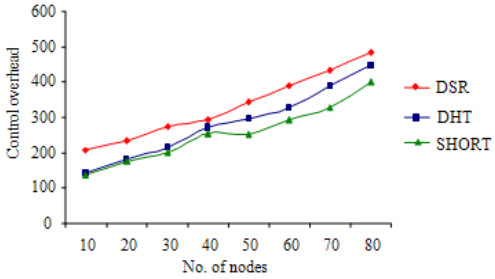

Fig. 5: No. of nodes and control overhead

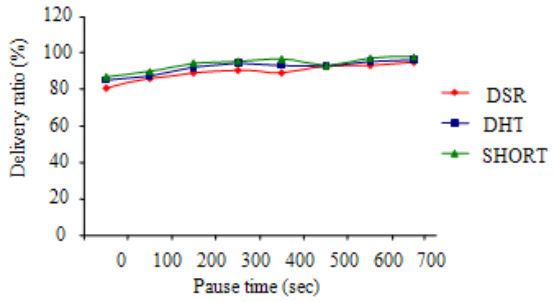

Fig. 6: Pause time and delivery ratio

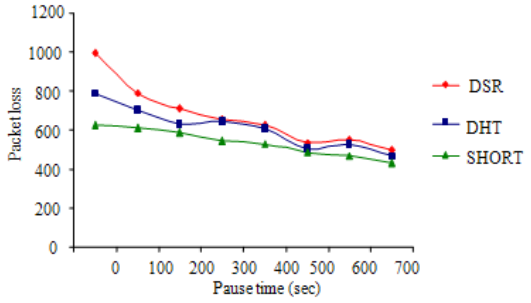

Fig. 7: Pause time and packet loss

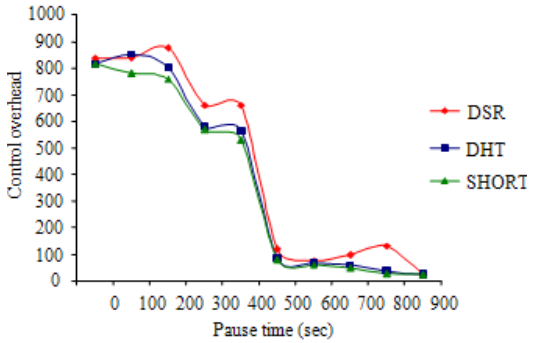

Fig. 8: Pause time and control overhead

Figure 7 shows the Pause Time Vs Packet Loss (Duraiswamy and Vijayaragavan, 2010) for DSR, Dual Hash Technique and SHORT. Here packet loss in DHT and SHORT decreases due to the increase in pause time. Packet loss has been reduced to 2.4% in DHT and 7.8% in SHORT when compared to DSR (Al-Hunaity *et al*., 2007).

Figure 8 shows the Pause Time Vs Control Overhead for DSR, Dual Hash Technique and SHORT. Here the control packets decrease when the pause time increases. SHORT has 5.5% less control packets compared to DSR and 2.9% less that of DHT.

DISCUSSION

Dual Hash Technique (DHT) along with SHORT has been studied and its performance is analyzed using NS-2 simulator. DHT along with SHORT has been applied to DSR routing protocol and its performance has been measured. The difference performance metrics analysed are packet delivery ratio, control overhead and packet loss for DSR, DSR-Dual Hash Technique, DSR-DHT-SHORT. The security has improved in DHT-SHORT when compared to DSR.

CONCLUSION

As the technology for ad hoc wireless networks gains maturity, comprehensive security solutions based on realistic trust models and addressing all prevalent issues like routing key management and cooperation enforcement are expected to appear. The solutions presented in this study only cover a subset of threats and are far from providing a comprehensive answer to the security problem in ad hoc networks. This study analyses the performance of the DSR protocol with the application of Dual Hash Technique in association with SHORT. This study could be extended to other protocols like TORA.

REFERENCES

Alandzi, V. and A. Quintero, 2007. Proximity aware routing in ad hoc networks. J. Comput. Sci., 3: 533-539. DOI: 10.3844/jcssp.2007.533.539

Al-Bdour, H.S., 2005. An adaptive routing algorithm for ad hoc mobile networks. J. Comput. Sci., 1: 215-220. DOI: 10.3844/jcssp.2005.215.220

Alfawaer, Z.M., G. Hua and N. Ahmed, 2007a. A novel multicast routing protocol for mobile ad hoc networks. Am. J. Applied Sci., 4: 333-338. DOI: 10.3844/ajassp.2007.333.338

Alfawaer, Z.M., G. Hua and N.A. Hamdeh, 2007b. Utilization of AODV in wireless ad hoc networks. J. Comput. Sci., 3: 218-22. DOI: 10.3844/jcssp.2007.218.222

Al-Hunaity, M.F., S.A. Najim and I.M. El-Emary, 2007. A comparative study between various protocols of manet networks. Am. J. Applied Sci., 4: 663-665. DOI: 10.3844/ajassp.2007.663.665

Barati, A., A. Movaghar, H. Barati and A.A. Mazreah, 2008. Decreasing overhead and power consuming in ad-hoc networks by proposal a novel routing algorithm. J. Comput. Sci., 4: 427-436. DOI: 10.3844/jcssp.2008.427.436

Bhalaji, N., S. Banerjee and A. Shanmugam, 2008. A novel routing technique against packet dropping attack in adhoc networks. J. Comput. Sci., 4: 538-544. DOI: 10.3844/jcssp.2008.538.544

Duraiswamy, K. and S. Vijayaragavan, 2010. An analysis of power aware congestion control multipath multicast protocol for mobile ad hoc network. J. Comput. Sci., 6: 1381-1388. DOI: 10.3844/jcssp.2010.1381.1388

Hanapi, Z.M., M. Ismail and K. Jumari, 2009. Priority and random selection for dynamic window secured implicit geographic routing in wireless sensor network. Am. J. Eng. Applied Sci., 2: 494-500. DOI: 10.3844/ajeassp.2009.494.500

Hao, Y., L. Haiyun, Y. Fan, Z. Lixia and S. Lu, 2004. Security in mobile ad hoc networks: Challenges and solutions, IEEE Wireless Communi., 11: 38-47. DOI: 10.1109/MWC.2004.1269716

Isaac, J.T., S. Zeadally and J.S. Camara, 2010. Security attacks and solutions for vehicular ad hoc networks. IET Commun., 4: 894-903. DOI: 10.1049/iet-com.2009.0191

Jayakumar, G. and G. Gopinath, 2007. Ad hoc mobile wireless networks routing protocols-a review. J. Comput. Sci., 3: 574-582. DOI: 10.3844/jcssp.2007.574.582

Khatri, P., M. Rajput, A. Shastri and K. Solanki, 2010. Performance study of ad-hoc reactive routing protocols. J. Comput. Sci., 6: 1159-1163. DOI: 10.3844/jcssp.2010.1159.1163

Koul, A., R.B. Patel and V.K. Bhat, 2008. Arithmetic encoding based dynamic source routing for ad-hoc networks. J. Comput. Sci., 4: 353-359. DOI: 10.3844/jcssp.2008.353.359

Liu, K., J. Deng, P.K. Varshney and K. Balakrishnan, 2007. An acknowledgment-based approach for the detection of routing misbehavior in manets. IEEE Trans. Mobile Comput., 6: 536-550. DOI: 10.1109/TMC.2007.1036

Mallah, R.A. and A. Quintero, 2009. A light-weight service discovery protocol for ad hoc networks. J. Comput. Sci., 5: 330-337. DOI: 10.3844/jcssp.2009.330.337

Murugan, R. and A. Shanmugam, 2010. A combined solution for routing and medium access control layer attacks in mobile ad hoc networks. J. Comput. Sci., 6: 1416-1423. DOI: 10.3844/jcssp.2010.1416.1423

Patel, R.B. and N. Goel, 2006. Mobile agents in heterogeneous networks: A look on performance. J. Comput. Sci., 2: 824-834. DOI: 10.3844/jcssp.2006.824.834

Peng, F. and Z. Deyun, 2006. Hybrid optimize strategy based qos route algorithm for mobile ad hoc networks. J. Comput. Sci., 2: 160-165. DOI: 10.3844/jcssp.2006.160.165

Pirzada, A.A., C. McDonald and A. Datta, 2006. Performance comparison of trust-based reactive routing protocols. IEEE Trans. Mobile Comput., 5: 695-710. DOI: 10.1109/TMC.2006.83

Safdar, G.A., C. McGrath and M. McLoone, 2006. Existing wireless network security mechanisms and their limitations for ad hoc networks. Proceedigns of the Irish Signals and Systems Conference, June 28-30, IEEE Xplore, Dublin, pp: 197-202.

Sanzgiri, K., D. LaFlamme, B. Dahill, B.N. Levine and C. Shields *et al*., 2005. Authenticated routing for ad hoc networks. IEEE J. Select. Areas Commun., 23: 598-610. DOI: 10.1109/JSAC.2004.842547

Vijayaragavan, S., K. Duraiswamy, B. Kalaavathi and S. Madhavi, 2009. A performance study of reactive multicast routing protocols in virtual class room using mobile ad hoc network. J. Comput. Sci., 5: 788-793. DOI: 10.3844/jcssp.2009.788.793

Yampolskiy, R.V. and V. Govindaraju, 2007. Computer security: A survey of methods and systems. J. Comput. Sci., 3: 478-486. DOI: 10.3844/jcssp.2007.478.486

Zabian, A., A. Ibrahim and F. Al-Kalani, 2008. Dynamic head cluster election algorithm for clustered ad-hoc networks. J. Comput. Sci., 4: 42-50. DOI: 10.3844/jcssp.2008.42.50

Zhang, L., Q. Wu, A. Solanas and J. Domingo-Ferrer, 2010. Scalable robust authentication protocol for secure vehicular communications. IEEE Trans. Vehic. Technol., 59: 1606-1617. DOI: 10.1109/TVT.2009.2038222