International Journal of Information Processing, 10(2), 62-70, 2016
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Security of Zone Routing Protocol using HMAC-SHA512 Algorithm

Ravilla Dillil[a], Putta Chandra Shekar Reddy[b]

[a]Department of Electronics and Communication Engineering, Manipal Institute of Technology, Manipal University, Manipal 576 104 India, Contact: dilli.ravilla@manipal.edu

[b]JNTUH, Hyderabad, India, Contact: drpcsreddy@gmail.com.

Hash functions are used in information security applications for the generation and verification of digital signatures, key derivation, and pseudorandom bit generation. Hash algorithms are secure because, for a given algorithm, it is computationally infeasible to find a message that corresponds to a given message digest, or to find two different messages that produce the same message digest. Any change to a message will result in a different message digest with a very high probability. This will result in a verification failure when the secure hash algorithm is used with a digital signature algorithm or a keyed-hash message authentication algorithm. In our work, first we implemented the Zone Routing Protocol (ZRP), a hybrid MANET protocol is being implemented in Network Simulator 2 (NS2) and a hashing algorithm, keyed-Hash Message Authentication Code Secure Hashing Algorithm 512 (HMAC-SHA512) is implemented for the Authentication and Data Integrity of the information being sent. In addition to that a Trust-Based system is formulated for preventing the Denial-of-Services (DoS) Attacks. The first part of this paper introduces the HMAC-SHA512 for ensuring that the data packets are received by the destination only and in its original form but at the expense of the increased processing time at the source and the destination. The second part uses the Trust-Based system with those nodes that act maliciously being broadcasted in the network and isolated to render a higher throughput and packet delivery fraction but at the expense of the increased end to end delay.

Keywords : Denial-of-Service (DoS), Hash Algorithms, MANET, Message Authentication Code, NS2 Simulator, Trust based System, Zone Routing Protocol.

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are more prone to security threats than fixed-networks. In a MANET, a security problem can occur at any network layer and it includes data integrity attacks, by accessing, modifying, or injecting traffic; There are several approaches to provide security at the network layer level where routing is major aspect [1][2]. In this paper, we have used Hash Algorithms to address the security threats in Routing the information from one node to the other. A Hash function (H) maps a variable-length message (M) into a fixed-length message digest also called as Hash code (h) where h= H (M). In Secure Hash Algorithms, the compression function is specially designed for the hash function. The objective of using hash function is to provide Data integrity. We have family of Security Hash Functions as SHA-0, SHA-1, SHA-2 and SHA-3 [3].

Based on the algebraic way, Wang [4] showed the first attack in 1997 on SHA-0 and they proved that collisions can be found with complexity of 258. In 1998, Chabaud and Joux independently found the differential attack for SHA-0. It is also shown that SHA-1is suffering with collision attacks within 269 hash computations [1]. It was the first attack on the complete 80-step SHA-1 with in the complexity of 280 theoretical limit [4]. As we have these limitations for SHA-0 and SHA-1, is time to implement all security systems using SHA-2 and SHA-3 groups of algorithms. Figures 1 and 2 represent the basic definition of Hash functions.

Table 5
Simulation Parameters

Parameter	Value
Protocol	ZRP
Type of Attack	Packet Dropping
Duration	50sec
Simulation Area	1000m X 1000m
Propagation Model	Two ray Ground Reflection
Number of nodes	50
Channel	Wireless
MAC Protocol	IEEE 802.11
Antenna	Omnidirectional
Interface Queue	50 Packets
Mobility Model	Random way Point
Pause Time	20 sec
Zone Radius	5
Number of connections	90 CBR (TCP)
Malicious nodes	5 , 10 , 15 , 20 , 25
Transmission range	250m
Speed	10 - 100 m/s
Data Rate	2Mb

With the above parameters, the analysis is done and the performance parameters are evaluated as given in Table 5.

Table 6
Analysis of ZRP Without Trust-Based System

Percentage of Malicious Nodes	Throughput [in Kbps]	E2E Delay [in milli sec]	PDF
0	358.12	154.982	0.9404
10	352.23	192.198	0.8218
20	344.18	205.260	0.7414
30	338.14	224.141	0.6816
40	294.22	242.162	0.5207
50	189.18	267.154	0.3564

From Tables 6 and 7, we can see that the Packet Delivery fraction of the ZRP without trust when compared to that of with trust, the one with the trust based system performs better as it takes into consideration of the malicious nodes in the network. The initial PDF is never 100 percent as some packets are lost due to mobility. Thus the ZRP with trust rather than taking the shortest path also takes into consideration the behavior of the nodes. From the Tables 6 and 7, we can see that the end to end delay for the trust based system increases as the time taken to traverse the same distance (in hops) increases as compared to the conventional ZRP without trust. Finally, from Tables 6 and 7, we expect the Throughput to increase for the trust based system but as mobility and alternative path of communication comes into picture, the Throughput shows deviation from the theoretical results.

Table 7
Analysis of ZRP With Trust-Based System

Percentage of Malicious Nodes	Through put [in Kbps]	E2E Delay [in milli sec]	PDF
0	352.16	188.173	0.9625
10	355.29	255.254	0.9216
20	354.43	256.216	0.7548
30	348.44	344.249	0.7224
40	338.83	318.853	0.7251
50	335.66	320.481	0.6028

4. CONCLUSIONS AND FUTURE SCOPE

In our work, the routing approach in mobile ad hoc networks with respect to the security is considered and analyzed the various threats against hybrid routing in ad hoc networks and proposed the requirements which are essential to be addressed for secure routing. In this paper two techniques namely HMAC-SHA512 for providing data integrity along with authentication and Trust-Based system to make the network more secure by preventing Denial of Service attacks in the network are used. Our proposed protocol reaches a better result towards accomplishing the security goals such as message integrity and message authentication, by taking a unified approach of digital signature. Along with cryptography based solutions, a Trust Based solution is also implemented which is based on the deportment of the nodes.

The first part of the paper is implementation of HMAC-SHA512 on to the existing ZRP which provides us data integrity and authentication but at the expense of the increased processing delay. The other part being the implementation of the Trust Based system that considers the malicious nodes of the network and tries to avoid them as these nodes affects the Packet Delivery Fraction (PDF). The Trust Based system increases the PDF but at the expense of the increased End to End Delay. The simulations further show that as the malicious nodes percentage goes past 30 percent, the performance of the system degrades considerably.

The future possible extension of our work may include employing additional feature to SZRP so that it can handle a scenario where the data is also confidential between the source and the destination and there are some safeguards against any attack to the data privacy (confidentiality). This implementation will increase the scope of the work to the military level operations where we need the security as well as privacy against the eavesdropping attacks. In addition one can implement a secure key exchange mechanism so that multiple nodes can communicate in the network simultaneously in a secure manner without the prior knowledge to the secret key amongst the source S and Destination D.

REFERENCES

1. X Wang, Y Lisa Yin and Hongbo Yu. Finding Collisions in the Full SHA-1. *in Conference Proceedings of Crypto*, 3621:17-36, 2005
2. C Lee. A Study on Effective Hash Routing in MANET. *Advanced Science and Technology Letters*, 95, 47–54.
3. Radha S S, S V Dhopte. The Secure Dynamic Source Routing Protocol in MANET using MD5 Hash Function. *IJEIR* , 1(3), 2012.
4. Y Huang, W Lee. A Cooperative Intrusion Detection System for Ad Hoc Networks. *in Proceedings of the 1st ACM Workshop Security of Ad Hoc and Sensor Networks Fairfax, Virginia*, 2003.
5. B Carbunar, C Nita-Rotaru. JANUS: A Framework for Scalable and Secure Routing in Hybrid Wireless Networks. *IEEE Transactions on Dependable and Secure C0mputing*, 6(4), 2009.
6. Md T Rahman, Md J N Mahi. Proposal for SZRP Protocol with the Establishment of the Salted SHA-256 Bit HMAC PBKDF2 Advance Security System in a MANET. *in Proceedings of International Conference on Electrical Engineering and Information and Communication Technology (ICEEICT)*, 2014.

Dilli Ravilla received the BTech. Degree in Electronics and Communication Engineeringfrom JNTUH, Hyderabad, India, in 2003 and the ME Degree in Electronics and Communication Engineering from Satyabama University, Chennai, India, in 2006. He is working toward the Ph.D Degree in the Electronics and Communication Engineering at JNTUH University, Hyderabad, India. Currently, he is working as faculty in Electronics and Communication Department in MIT, Manipal University, Manipal, India. His research interests include Ad-hoc Network Routing. His research has focused on the Design of Hybrid Routing Protocols and its Effects on Performance Optimization in Ad-hoc Networks.

Chandra Shekar Reddy Putta received the BTech. Degree in Electronics and Communications Engineering from JNTUH, Hyderabad, India and ME from Bharatiyar Deemed University. He received MTech and Ph.D from JNT University. Hyderabad, India. He joined as faculty in JNTU, Currently, he is working as Professor in JNTUH, Hyderabad, India. He is an author of numerous technical papers in the fields of High-Speed Networking and Wireless Networks. His research interests include Mobile and Wireless Communication and Networks, Personal Communication Service and High-Speed Communication and Protocols.