ISSN: 2321-7782 (Online)
Volume 2, Issue 8, August 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Securing AODV Protocol using Signature Based Techniques

Pratik Buchke[1]
Department of IT
O.I.S.T.
Bhopal – India

Prof. Vineet Richharya[2]
Department of CSE
LNCT
Bhopal – India

Abstract: ***In Ad hoc network all nodes are mobile and can be connected dynamically in an arbitrary manner. No default router is available for routing. Since in an ad hoc network, a significant concern is the ability to route in the presence of Byzantine failures which include nodes that drop, fabricate, modify, or mis-route packets in an attempt to disrupt the routing service. As Byzantine fault occur in Ad-hoc On-Demand Distance Vector (AODV) protocol. In this paper, we propose three methods for securing AODV protocol from Byzantine attacks by using Signature based techniques. These techniques are CME (Combine Message Encryption), CEM (Combine Encrypted Message) and ASM (Aggregate Signature of Messages). Finally, we compare our approach with AODV protocol. The results shown that the quality of service has been improved based on three parameters (delay, network load and throughput).***

Keywords: Ad-hoc; Networks; Protocols.

I. INTRODUCTION

Mobile ad-hoc wireless networks hold the promise of the future, with the capability to establish networks at anytime, anywhere. These networks don't rely on extraneous hardware which makes them an ideal candidate for rescue and emergency operations. These networks are built, operated and maintained by its constituent wireless nodes. These nodes generally have a limited transmission range and so each node seeks the assistance of its neighboring nodes in forwarding packets. In order, to establish routes between nodes, which are farther than a single hop, specially configured routing protocols are engaged. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology. These protocols can by far and large be categorized into two main types: Reactive and Proactive [1]. The nodes in an ad-hoc network generally have limited battery power and so active routing protocols endeavor to save upon the same, by discovering routes only when they are essentially required. In contrast, proactive routing protocols establish and maintain routes at all instants of time, so as to avoid the latency that occurs during new route discoveries. Both types of routing protocols require persistent cooperative behavior, with intermediate nodes primarily contributing to the route development. Similarly each node, which practically acts like a mobile router [1], has absolute control over the data that passes through it. In essence, the membership of any adhoc networks indisputably calls for sustained depiction of benevolent behavior by all participating nodes. However, this is more than often difficult to achieve in an open environment and so these networks are frequently attacked by malicious nodes, which may originate internally or join externally. Two kinds of attacks can be launched against ad-hoc networks [2], Passive and Active. In passive attacks the attacker does not disturb the routing protocol. It only eavesdrops upon the routing traffic and endeavors to extract valuable information like node hierarchy and network topology from it. In active attacks, malicious nodes can disturb the correct functioning of a routing protocol by modifying routing information, by fabricating false routing information, and by impersonating other nodes[3].

Cryptographic mechanisms are commonly used to protect routing protocols by enforcing mutual trust relationships among the wireless nodes [4]. Security in mobile ad-hoc wireless networks is a two-fold problem. One is the security of the routing protocols that enable the nodes to communicate with each other and the second is the protection of the data that traverses the

network on routes established by the routing protocols. In this paper, after Introduction in Section I, we describe some recent secure routing protocols for ad-hoc networks in Section II, which have been developed to counter known attacks. In Section III we propose a scheme for securing the Ad-hoc On-Demand Distance Vector routing protocol. A security analysis of the proposed scheme is presented in Section IV with concluding remarks in Section V.

II. PREVIOUS WORK

Routing protocols have been tested for wireless mesh networks in past, but for some other conditions. Definitely routing protocols in WMNs have been tested for delay, throughput also but in our paper three different parameters (delay, throughput and network load) is tested together for the first time, and its simulation has been done on OPNET Modeler 14.0.

Monis Akhlaq [5] focuses on achieving the routing and secure data exchange in a single step. This will facilitate the user nodes to perform routing, mutual authentications, generation and secure exchange of session key in one step thus ensuring confidentiality, integrity and authentication of data exchange in a more suitable way.

Nital Mistry [6] focuses on analyzing and improving the security of Ad-hoc On Demand Distance Vector (AODV) routing protocol against Blackhole Attacks.

Shidi Xu [7] propose a comparatively efficient scheme to perform ARAN protocol, based on AODV, by using onetime signature in place of conventional signature, aiming at achieving the same level of security but improved efficiency.

Kimaya Sanzgiri [8] provides a solution for securing routing in the managed-open environment. ARAN provides authentication and non-repudiation services using predetermined cryptographic certificates that guarantees end-toend authentication.

Yiling Wen [9] presents a new aggregate signature. Its pairing operations are independent of the number of signers. It is more efficient than other previous scheme. They propose a new aggregate signature scheme from bilinear pairings

Asad Amir Pirzada [10] presented a scheme for securing the Ad-hoc On-Demand Distance Vector routing protocol used in mobile ad-hoc wireless networks. The secure AODV protocol provides requisite measures for protection of route discovery and transfer of data.

III. SECURING THE AD-HOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL

The goal of this work is to provide routing survivability under an adversarial model where any intermediate node or group of colluding nodes can perform Byzantine attacks such as creating routing loops, misrouting packets on non-optimal paths, or selectively dropping packets; only the source and the destination nodes are assumed to be trusted. To our knowledge, there is no on-demand wireless routing protocol addressing Byzantine failures, particularly in a model where attackers can collude. In this paper, we present three techniques that are based on aggregate signatures, as opposed to chained digital signatures. This approach provides stronger security guarantees and improved convergence times.

Aggregate Signatures:

Given n users that sign n messages, an aggregate signature allows the composition of these digital signatures into a single short signature. An aggregate signature only verifies correctly if the verifier is provided with the exact contents signed by, and the exact identity of, every party that contributed to the aggregate. It is important to note that the aggregation can be performed incrementally; in our scenario, if a node receives signature σ12 (obtained by aggregating σ 1 and σ 2), then it can further aggregate it with σ 3 to obtain σ 123. Furthermore, given an aggregate signature, it is cryptographically difficult to remove the contribution of one of the signers without knowledge of their private key.

Proposed Algorithm for Signature Techniques

A. Common Message Encryption (CME)

In a CME scheme, messages are generated by individual users. They can then be combined and signature is generated by some aggregating party. The aggregating party need not be one of the users, and need not be trusted by them. The CME algorithm takes as input respective messages M1; : : : ;Mn under respective public keys PK1; : : : ;PKn. (The assignment of indices is arbitrary.) It outputs a single signature σ.

The aggregate verification algorithm, given an signature σ, messages M1; : : : ;Mn, and public keys PK1……PKn, verifies that σ is a valid signature on the given messages under the given keys.

B. Common Encrypted Message (CEM)

In a CME signature scheme, signatures are generated by individual users. They can then be combined into an aggregate signature by some aggregating party. The aggregating party need not be one of the users, and need not be trusted by them. Every aggregate signature scheme is a generalization of an ordinary signature scheme. An aggregate signature is the same length as an ordinary signature in the underlying scheme.

The aggregation algorithm takes as input signatures s1…….sn on respective messages M1……Mn under respective public keys PK1…..PKn. (The assignment of indices is arbitrary.) It outputs a single aggregate signature s.

The aggregate verification algorithm, given an aggregate signature s, messages M1…….Mn, and public keys PK1…….PKn, verifies that s is a valid aggregate signature on the given messages under the given keys.

C. Aggregate Signature of Messages (ASM)

In an ASM signature scheme, signature is generated by first user. This signature then combines with the next message. Then second user create signature of its own message and received signature. This process continues up to n user. Every aggregate signature scheme is a generalization of an ordinary signature scheme.

The aggregation algorithm takes as input M1 under respective public key PK1 and creates outputs a single aggregate signature σ1. For second user algorithm takes input as M2 and σ1 under respective public key PK2 and creates outputs a single aggregate signature σ2. This process continues up to n user.

The aggregate verification algorithm, given an aggregate signature σ, messages M1…….Mn, and public keys PK1…….PKn, verifies that σ is a valid aggregate signature on the given messages under the given keys.

Nodes	Parameters	AODV	SAODV using CME	SAODV using CEM	SAODV using ASM
15	Delay (sec)	0.011	0.00851	0.00852	0.015
	Network Load (bits/sec)	1,860,000	1,50,000	410,000	1,880,000
	Throughput (bits/sec)	1,920,000	225,000	490,000	1,950,000
30	Delay (sec)	0.0145	0.011	0.01	0.012
	Network Load (bits/sec)	2,510,000	159,000	401,000	2,050,000
	Throughput (bits/sec)	2,710,000	590,000	625,000	2,270,000
60	Delay (sec)	0.0171	0.0211	0.0162	0.0142
	Network Load (bits/sec)	2,310,000	182,000	450,000	2,250,000
	Throughput (bits/sec)	3,210,000	2,250,000	2,250,000	3,100,000

Table 1. Performance of routing approaches.

IV. SECURITY ANALYSIS

In this section we discuss how the presented security scheme defies possible attacks in an ad-hoc network. As discussed earlier, the basis of a security infrastructure is primarily dependent on the initial key exchange providing authentication. Other security services like confidentiality, integrity and no repudiation all rely on the accuracy of the authentication service. Key revocation, being an important issue has not been addressed in the scope of this paper, primarily because it requires the presence of an omnipresent, and often omniscient, trust authority, which we have already deemed inappropriate for such a dynamic environment. We now discuss how this scheme satisfies the seven requirements of any secure routing protocol:

A. Authorized nodes to perform route computation and discovery

The authentication and key exchange protocol ensures that only authorized nodes are able to perform the route discovery. As the routing control packets are encrypted and authenticated by each forwarding node, malicious nodes will not be able to create fallacious routing packets.

B. Minimal exposure of network topology

As all routing information is encrypted between nodes, an adversary will gain no information regarding the network topology from passive eavesdropping.

C. Detection of spoofed routing messages

Spoofing of either the MAC or IP addresses does not provide any benefit to the adversary until the time the authentication protocol is assumed to be secure. As the initial authentication links a number of identities to each node's private key, the spoofing node will have to create a similar private key prior to launching any attack.

D. Detection of fabricated routing messages

Malicious nodes cannot inject fabricated routing messages into the network as each routing packet is secured through an encryption key, which provides the benefit of confidentiality, authentication and integrity at the same time. To fabricate a routing message the session key needs to be compromised, which is not possible until the time the key exchange protocol is assumed to be secure.

E. Detection of altered routing messages

Routing messages are relayed between the nodes in an unintelligible format. If the symmetric cipher also provides the integrity then the alteration of routing messages is virtually impossible. Addition of a keyed hash for better integrity checking may be considered only after a cost benefit analysis.

F. Avoiding formation of routing loops

The proposed scheme ensures that routing loops cannot be formed through malicious action. Routing loops usually occur if a malicious node is able to spoof, alter or fabricate legitimate routing packets.

G. Prevent redirection of routes from shortest paths

Shortest paths are created usually by decrementing the number of addresses in the source routing protocol. The scheme is designed in such a manner that routing packets are only accepted from authenticated immediate neighbors. This ensures that an adversary cannot inject such routing packets unless an authorized node first authenticates it.

V. CONCLUSION

In this paper we have presented a scheme for securing the Ad-hoc On-Demand Distance Vector routing protocol used in mobile ad-hoc wireless networks. The secure AODV protocol provides requisite measures for protection of route discovery and

transfer of data. These measures can be exercised independently without a central trust authority with nodes negotiating session keys independently. All signature based techniques are simulated in OPNET Modeller14.0.

ACKNOWLEDGEMENT

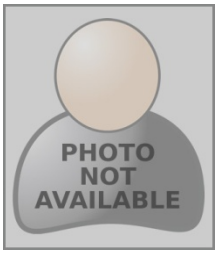
Overall our paper focus on malicious nodes trying to launch passive or active attacks against the network is thwarted through efficient key verification mechanisms and a multilayered enciphering scheme. To highlight its viability we have discussed its resistance to a number of attacks specific to ad-hoc networks.

References

1. Md. Saiful Azad, Farhat Anwar, Md. Arafatur Rahman, Aisha H.Abdalla, Akhmad Unggul Priantoro and Omer Mahmoud "Performance Comparision of Proactive and Reactive Multicast Routing Protocols over Wirerless Mesh Networks", IJCSNS June 2009, pp 55-62
2. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto and Nei Kato "A Survey Of Routing Attacks in Mobile Adhoc Network" IEEE Conference October 2007, pp 85-91
3. Suman Deswal and Sukhbir Singh "Implementation of Routing Security Aspects in AODV" IACSIT journal, vol-2 February 2010 pp. 135-138
4. Rashid Hafeez Khokhar, Md Asri Ngadi, Satria Mandala. "A Review Of Routing Attacks in Mobile Adhoc Network" IJCSS Journal, Vol.2, pp. 18-29
5. Monis Akhlaq, M Noman Jafri, Muzammil A Khan, and Baber Aslam "Addressing Security Concerns of Data Exchange in AODV Protocol", 2006, pp 29-33
6. Nital Mistry, Devesh C Jinwala, Mukesh Zaveri "Improving AODV Protocol against Blackhole Attacks " IMECS 2010
7. Shidi Xu, Yi Mu and Willy Susilo "Authenticated AODV Routing Protocol Using One-Time Signature and Transitive Signature Schemes ",2006 pp. 47-53
8. Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth, M. Belding-Royer "A Secure Routing Protocol for Ad Hoc Networks", 2002
9. Yiling Wen, Jianfeng Ma," An Aggregate Signature Scheme with Constant Pairing Operations ",2008 pp.830-833
10. Asad Amir Pirzada "Secure Routing with the AODV Protocol ",2005 pp.57-61

AUTHOR(S) PROFILE

Pratik Buchke received the M.Tech degree in Computer Science & Engineering from LNCT, Bhopal (MP) in 2010 and BE degree in Information Technology from TRUBA, Bhopal (MP) in 2006. His research area ad-hoc network, cloud computing, database management. Currently working as Assistant Professor in Department of Information Technology in OIST, Bhopal (MP).



Prof. Vineet Richharya received the PHD degree in Computer Science & Engineering 2013 MTech degree in Computer Science & Engineering in 2000 & BE degree in Computer Science & Engineering in 1990. His research area Image Processing, ad-hoc network, cloud computing. Currently working as Professor in Department of Computer Science & Engineering, LNCT, Bhopal (MP).

