IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-2 E-ISSN: 2347-2693

Comparative on AODV and DSR under Black Hole Attacks Detection Scheme Using Secure RSA Algorithms in MANET

Meenakshi Jamgade[1*] and Vimal Shukla [2]

[1*] *Dept. of Computer Science and Engineering, RGPV, India*
[2] *Dept. of Computer Science and Engineering (KNP Bhopal), India*

www.ijcseonline.org

Received: Feb /02/2016 Revised: Feb/09/2016 Accepted: Feb/21/2016 Published: Mar/29/ 2016

Abstract*— Mobile Ad hoc Network (MANET) is a new field of communication operating in an extremely unpredictable and dynamic environment. These networks are gaining increasing popularity in recent years because of their ease of deployment. A MANET consists of collection of wireless mobile nodes that are capable of communicating with each other without the use of any network or any centralized administration. In ad hoc networks, routing protocols are challenged with establishing and maintaining multi-hop routes with security in the face of mobility, bandwidth limitation and power constraints. In particular in MANET, any node may be compromise the routing protocol functionality by disrupting the route discovery process. To achieve broad protection and desirable network performance, routing security is unavoidable. In this research work, a secure routing protocol for MANET is designed with the countermeasures to reduce or eliminate different types of security vulnerabilities and attacks. This paper provides routing security to the Ad hoc on demand Distance Vector (AODV) routing protocol by eliminating the threat of Black Hole attack, Wormhole attack, Rushing attack, and Impersonation attack. The proposed solutions are tested using Network Simulator2 (NS2), a scalable network simulator. The performance is studied for in various routing parameters such as packet delivery ratio, average end - to - end delay and routing overhead and are compared with the AODV and DSR. Hence we have known Cryptographic algorithm such as RSA (Rivest Shamir Adleman) Algorithm is used for providing a secure routing between mobile nodes even in the presence of malicious nodes .In brief, this paper presents a counter measure to overcome Black hole attack.

Keywords*— Wireless Ad-Hoc Network, Blackhole Attack, Tunnel, Performance Analysis, Routing Protocol, MANET Security.

1. INTRODUCTION

The Mobile Ad-hoc Networks (MANETs) are part of today's revolution in technology. MANETs are groups of wireless devices and nodes that communicate by dispatching packets to others or on behalf of another device/node, without a central network authority and infrastructure controlling data routing. In MANETs, each node acts as router/network manager for other nodes. MANETs are vulnerable due to their basic characteristics which include topological changes, no point of network management, restriction of resources, no certifiable or centralized authority, etc. Threats to personal and company privacy, and assets by attacks upon networks and computers continue in spite of efforts of network administrators and IT vendors to safe as environments. Secured transmission and communication in MANET is a major challenge as this network is open to many types of attacks. Understanding probable security attacks to MANETs is a serious issue as they are targeted by attacks including Flooding attack, Wormhole attack, Black hole attack, Denial of Service (DoS), Selfish-node misbehaving, Routing table overflow attack, Impersonation attack, etc. Earlier studies reveal the different attack categories on MANETs like Passive/Active attacks, Internal/External attacks and Routing and Packet Forwarding attacks. Some of the attacks aim at single nodes and others aim at multiple nodes. Malicious and selfish nodes are other types of attack which severely degrade the security and performance of the network.

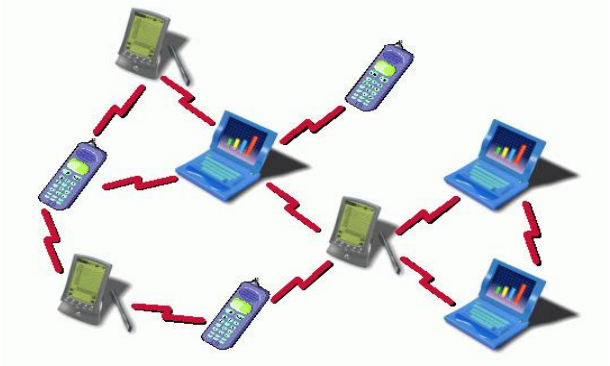

Figure 1: Mobile Ad hoc Network

1.1 ROUTING PROTOCOLS

To ensure delivery of packets from sender to destination in ad-hoc networks, a node must create a routing protocol and maintain the related routing tables in memory. Routing protocols can be categorized as reactive, proactive, and hybrid. As of date there are almost one hundred routing protocols, most of which are standardized by the Internet Engineering Task Force (IETF). This section gives an overview of the some of the important ones for each category.

1.1.1. Reactive protocols

Reactive protocols set up routes on-demand. When a node wants to communicate with another without a route, the routing protocol will try to create route and the Ad-Hoc on-Demand Distance Vector (AODV) routing protocol is one such protocol [1] (Perkins et al. 2003). The characteristic of an AODV is that the topology information is transmitted only on-demand by nodes. When a node transmits to a particular host of which it has no route, it will create a Route REQuest (RREQ) that is passed on to other nodes. This leads control traffic overhead to be dynamic which results in an initial delay when communication is initiated. A route is located when the RREQ reaches either the destination or an intermediate node with a valid route entry for the destination. The AODV remains passive when a route exists between end points. When the route either becomes invalid or lost, the AODV will again issue a request.

1.1.2. Proactive protocols

A proactive approach to MANET routing requires a constant update on topology information. The entire network should be known to all nodes, in theory. This leads to a constant overhead in routing traffic without initial communication delays.

1.1.3. Hybrid protocols

Hybrid protocols combine both proactive and reactive approaches. The Zone Routing Protocol (ZRP) is an example [2] (Haas et al. 2002). This protocol divides topology into zones and uses different routing protocols within/between zones depending on their strengths and weakness. ZRP is modular and so any routing protocol can be used within and between zones. The zone size is defined by the parameter '*r*' which describes the radius in hops. Intra zone routing is through a proactive protocol as protocols keep updating views of zone topology and so there are no initial delays when communicating within zone nodes. Inter zone routing uses reactive protocol thereby eliminating the need for nodes to be proactively fresh in the entire network.

2. SYSTEM MODEL

SECURITY IN AD HOC NETWORKS

Apart from reliability and Quality of service, security is also an important requirement of ad hoc networks. Many of the applications of ad hoc networks are critical and cannot be deployed without granting a certain level of security. For example, in military applications, it is important that an adversary not be able to listen to the commands that are sent to the soldier, not to drop the commands so the other person doesn't know about it, not be able to inject false commands, and not replay legitimate commands. For certain applications that grant access to resources based on node's location, it is critical not to allow any intruder to gain access of the location information of the nodes. There are many such issues that have to be taken into account when a security protocol is designed for ad hoc networks.

There are several reasons that make security in ad hoc networks different and more challenging than wired networks. First, in ad hoc networks, the nodes use the wireless medium to communicate with each other. Thus, it is easy for an adversary to eavesdrop, modify or inject false packets as the medium is open instead of physically tapping into network wires to gain access. Moreover, in ad hoc networks there is no clear line of defense compared to wired networks where one can place the firewalls or gateways at the entry point into the network to prevent the illegitimate access. In addition, nodes in ad hoc networks also act as routers and are required to forward packets for other nodes in a multi hop manner. Thus a selfish or malicious node can choose to drop and not forward packets for others in order to either save its energy or to disrupt the network operation. There are many different aspects to consider in classifying the attacks in ad hoc networks. They can be classified into passive and active attacks depending on the involvement level of the attacker. In passive attack, attackers do not disrupt the routing operation but only eavesdrop in the network in order to learn valuable information like network

topology, traffic analysis and so on. In an active attack, on other hand, the adversaries can modify routing information to attract the traffic towards them, or they perform modification or deletion of messages, or they drop packets and so on.

Unlike passive attacks, the active attacks affect the normal functionality of the network. Another classification depends on the domain of the attack. This classifies attacks into internal and external attacks. An external attack is caused by the external nodes i.e., nodes that do not belong to the network. An internal attack is caused by the compromised node that already shares cryptographic keys with other nodes present inside the network and authenticated to participate in network operations. Usually, these attacks can cause more damage to the network compared to the external attacks that are performed by nodes that are not part of the network (Deng and Agarwal 2002, Zhou and Haas 1999). External attacks can be prevented by using any standard security mechanism. However internal attacks are very hard to detect, because it is launched by compromised nodes that have been authorized by the victim network. Depending on whether the attacker tries to hide his misbehaving actions, the attacks are classified into stealthy and non-stealthy attacks. Also, the attacks can be classified as cryptography and noncryptography related attacks. In cryptography related attacks the attacker tries to break the cryptographic protocols, for example, using brute force attack to find the key used in an encryption system. In non-cryptography related attacks the attacker will try to make use of the faults in routing protocol design without breaking the encryption system. The list of different attacks possible at each layer of the internet model is described in the Table 1 .

Table 1 Security attacks in each layer

Layers	Security Attacks
Application Layer	DOS attack, Repudiation and Data corruption
Transport Layer	TCP-SYN Attack, Session Hijacking
Network Layer	Wormhole attack, Blackhole attack, Gray Hole attack, Byzantine attack, Flooding attack, DOS attack, Location Disclosure attack
Data Link Layer	Traffic monitoring and Analysis, MAC misbehaving
Physical Layer	Jamming attack, Interference, Eavesdropping

Black Hole attack: In this attack [2] a malicious makes use of routing protocols to misrepresents that it is having the shortest and fresh enough route to destination without checking the availability of routes and drops the packets without forwarding further, thereby degrading network performance.

Wormhole Attack: In a wormhole attack [9], an attacker receives packets at one point in the network, tunnels them to another point in the network, and then replays them into the network from that point. Routing can be disrupted when routing control message are tunnelled. This tunnel between two colluding attacks is known as a wormhole.

Replay Attack: An attacker that performs a replay attack is retransmitted the valid data repeatedly to inject the network routing traffic that has been captured previously. This attack usually targets the freshness of routes.

Gray-hole attack: This attack is also known as routing misbehaviour attack which leads to dropping of messages. Gray hole attack [8] has two phases. In the first phase the node advertise itself as having a valid route to destination while in second phase, nodes drops intercepted packets with a certain conditions.

Flooding attack: In flooding attack [10] multiple RREQ'S are sent from void IP addresses if the scope of the IP address is known else random IP addresses are chosen and the network is flooded with a large number of RREQ'S hence, the name flooding. When flooding attack takes place in a particular route the data packets discover the secure route and reach the destination.

3. PREVIOUS WORK

[8] Gupta et al. (2011) analyzed MANET's Black hole attack with Proactive routing protocol i.e. OLSR and Reactive routing protocol AODV. Comparisons of Black hole attack for both protocols were considered. Attack impact on MANET performance is evaluated to learn which is more vulnerable and how much the attacks impact both protocols. The analysis is on performance metrics like throughput, network load and end to end packet delay. After many comparisons, Black Hole attack was analyzed with regard to parameters including end to end packet delay, throughput and network load.

[9] Zapata (2002) provides a summary of many approaches to security features in routing protocols in mobile ad-hoc networks (MANET) describing at the same time, secure AODV (an extension to AODV providing security features) with a summary of its operation and future enhancements. Two mechanisms secure AODV messages: digital signatures to authenticate a message non-mutable fields and hash chains to safeguard hop count information. Every node generating/forwarding route error messages) uses digital signatures to sign a full message verifiable by a neighbor receiving it.

[10] Khalil et al. (2005) presented A Lightweight Countermeasure for the Wormhole Attack in Multi hop Wireless Network (LITEWORP), a simple protocol to detect/mitigate wormhole attacks in ad-hoc and sensor wireless networks. It uses a secure two-hop neighbor discovery and monitors local control traffic to detect nodes involved in such attacks and also has a countermeasure which isolates malicious nodes from the network thereby doing with the chance of more damage.

[11] Kannhavong et al. (2008) proposed a unique acknowledgement between two hop neighbours whenever the control traffic was successfully received. The proposed methodology was able to protect the network from link spoofing, wormhole attack without requiring location information or the full topology of the network. The proposed system was able to achieve higher packet delivery ratio compared to standard OLSR.

4. PROPOSED METHODOLOGY

In this paper, a cryptographic approach has been proposed for secure routing to overcome black hole attack in MANETs. In this approach hop count is encrypted using famous well known RSA (Rivest Shamir Adleman) algorithm.

Black hole attack occurs in route discovery phase. Basically black hole attack is modification of hop and immediate response using sequence number in the field of RREQ.

In this paper we considered a scenario of 6 nodes with 2 phases of execution: In first phase one of the nodes is made malicious by modifying AODV routing protocol and in second phase traffic is made flow even in presence of malicious node just by encoding hop count since destination can decrypt it using RSA algorithm.

4.1 RSA Algorithm

RSA (Rivest Shamir Adleman) algorithm is public key cryptographic algorithm that makes use of 2 keys namely public key and private key [5].

If here RSA keys do not exist, they need to be generated. The key generation process is usually slow but it's performed seldom. It's involves three step: Key Generation, Encryption and Decryption [5].

Key Generation: Prime integers are used for key generation.

1. N=p*q
(N is used as modulus for both public key and private key)
2. Compute $\Phi(p*q) = (p - 1)*(q - 1)$.
3. Choose an integer e such that $1 < e < \Phi(p*q)$, and GCD of e and $\Phi(p*q)$ must be 1.
   - e is released as the public key exponent.
   - e having a short bit.

4. Determine **d** (using modular arithmetic) which satisfies congruence relation.

$d*e = 1 (\mathrm{mod}(\Phi(p*q))$

d is kept as the private key exponent

Encryption:

Destination node transmits it's public key (n, e) to Source node and keeps the private key secret then source wants to send message **M** to Destination.

It firstly turns **M** into an integer $0 < m < n$ by using an agreed-upon reversible protocol known as a padding schemes. It then computes the cipher text c corresponding to:

$C=m^d \pmod n$

Decryption:

Destination node can recover m from c by using its private key exponent d by the following computation:

$C=m^d \pmod n$

Given m, Destination can recover the original message **M** by reversing that padding scheme.

5. SIMULATION/EXPERIMENTAL RESULTS

All simulation experiments are developed and simulated on an Intel I3 machine using Ubuntu 12.04 LTS with 4 GB RAM and the network simulator NS2 version NS- 2.35.

In order to measure Packet Delivery Ratio and Routing Load, it is necessary to calculate total number of sent, received and forwarded AODV packets.

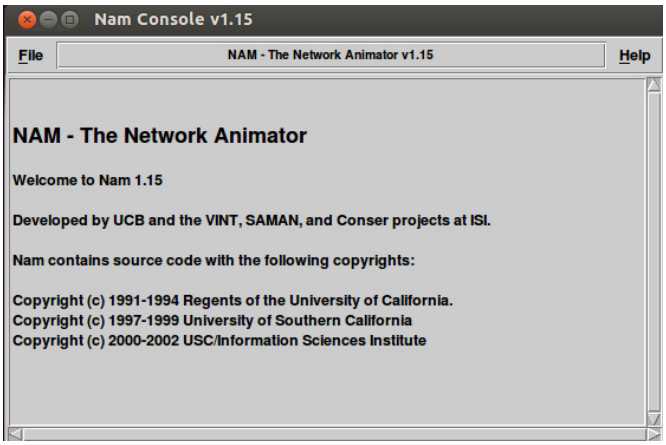

Figure 2: NAM Console in NS2

Table 2: The following parameters for simulation are used

Sr. No.	Parameter	Value
1	Simulator	NS 2.35
2	DoS Attack	Black hole Attack
3	Channel Type	Wireless channel
4	Antenna Type	Omni directional
5	The Protocol user	AODV,DSR
6	Underlying MAC Protocol	IEEE 802.11
7	Propagation Model	Two-Ray Ground
8	Queue	PriQueue
9	The number of Nodes Detected	Two or more node which are dropping packet
10	Nodes	10

6. CONCLUSION

In this paper, a survey on the blackhole attacks detection methods is made and found that to detect and prevent this attack mainly depends on the precise determination of the neighbouring information. Most of the detection methods are considered the neighbour case of the node. The countermeasures for the blackhole attack can be implemented at different layers.

Since current blackhole detection methods are imperfect, a sensor node will have a lot of false neighbours under large-scale blackhole attacks. Having many false neighbours often causes trouble for many protocols. A novel method for the routing security in Mobile Ad hoc Network using simple cryptographic algorithms is discussed. These proposed methodology was investigated on the performance of AODV and DSR with CBR traffic. The protocol performance with routing security is analyzed and observed that total control overhead is small for lower speed and increases to 64% more for higher speed than low mobility as the traffic in the network increases from 1 to 20. As a future work, the proposed algorithm is to be analyzed with respect to delay, speed and strength of the proposed algorithm.

7. FUTURE SCOPES

In future work, we can use better and fast routing strategy for path establishment and use effective fields for detecting packet. We can enhance the table entries at recipient to get the detection of pair of malicious nodes faster and improve conformance procedure.

REFERENCES

[1] Perkins and Royer,E. “Ad-hoc On-Demand Distance Vector Routing,” Second IEEE Workshop on Mobile Computer Systems and Applications, pp. 90-100, February 1999.

[2] Haas, Pearlman, and Samar. ZRP IEFT-MANET DRAFT, 5 Edition, July 2002.

[3] Razak, A. S., Furnell, M. and Brooke, P. J. "Attacks against Mobile Ad-hoc Networks Routing Protocols," 2004.

[4] Sanzgiri. K., LaFlammey, D., Dahilly,B.(2002). Authenticated Routing for Ad hoc Networks, IEEE, 2002

[5] Abbas, S., Merabti, M., Jones, D.L., Kifayat, K., Lightweight Sybil Attack Detection in MANETs, IEEE Systems Journal, Vol. 7, No. 2, 2013

[6] Guan, Q., Yu, F.R., Jiang, S., Joint Topology Control and Authentication Design in Mobile Ad Hoc Networks With Cooperative Communications, IEEE Transactions on vehicular technology, Vol. 61, No. 6, July 2012

[7] Ming-Yang, S. “Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems”, Computer communications, Vol.34, No.1, pp.107-117, 2010.

[8] Gupta, S., Gill, S. and Joshi, A. “Analysis of Black Hole Attack on AODV and OLSR Routing Protocols in MANET”, International journal of Computer application, Issue 1, Vol 1, pp. 11 – 19,October 2011.

[9] Zapata, M.G. “ Secure Ad-hoc On-Demand Distance Vector Routing”, Mobile Computing and Communications Review, Volume 6, Number 3, pp. 106 – 107.(2002).

[10] Khalil, Bagchi,S. andShroff,N.B. "LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks, in: International Conference on Dependable Systems and Networks (DSN), 2005, pp. 612–621.

[11] Kannhavong,B.,Nakayama,H., Nemoto,Y. and Kato, N."A Survey Of Routing Attacks In Mobile Ad-hoc Networks", IEEE Wireless Communications , pp. 85-91,October 2007.

[12] Putra, S. "An overview of mobile ad hoc networks for the existing protocols and applications", International journal on applications of graph theory in wireless ad hoc networks and sensor networks, Vol.2, No.1, pp.87-110, 2010.

[13] Rakesh kumar Sahu,Narendra S chaudhari "performance evaluation of ad hoc network under black hole attack 978-1-4673-4805- 8/$31.00, IEEE 2012

[14] Prasad lokulwar* and vivek shelkhe, "Security aware routing protocol for MANET using asymmetric cryptography using RSA algorithm", BIO-INFO Security Informatics ISSN: 2249-9423 &E-ISSN: 2249-9431, Volume 2, Issue 1, pp.-11-14. 2012.

[15] Kameswari Chebrolu *"NS2 Tutorial"* Dept. of Computer Science and Engineering, IIT Bombay.