

Security Issues and Performance Analysis for Ad Hoc on Demand Distance Vector Routing Protocol Networks

By

Dr. Brijesh Kr. Gupta, Tarun Chugh

Prof. & Head, Dept. of Computer Applications,

Galgotias College of Engineering & Technology, Greater Noida - 201 306, India,

Asst. Prof., Department of Info. Tech.

ITS Engineering College, Greater Noida – 201 306, India

profbkgupta@gmail.com

ABSTRACT

Mobile ad-hoc network is a relatively new innovation in the field of wireless technology. These types of networks operate in the absence of fixed infrastructure, which makes them easy to deploy at any place and at any time. Mobile ad-hoc networks are highly dynamic; topology changes and link breakage happen quite frequently. Therefore, we need a security solution, which is dynamic, too. Security in Mobile Ad hoc Networks (MANETs) is an important issue in need of a solution that not only works well with a small network, but also sustains efficiency and scalability. In ad hoc environment, much of the research has been done focusing on the efficiency of the network. Therefore, there are a number of routing protocols that provide good efficiency. Considering security has radically changed the situation, for all of the existing routing protocols are designed with an assumption that the participating players and the network environment do not harm the security. It highly contradicts with the reality. Most of the secure routing protocols have the various disadvantages. In this paper a trusted solution is provided for routing in ad hoc network. The routing protocol is modified by relating the security components. Finally, the simulation results of insecure AODV are studied using simulator.

Keywords:

AODV, Mobile Ad-hoc Networks, Packet Dropped, Secure Networks, Throughput.

1. INTRODUCTION

Mobile ad-hoc network is a relatively new innovation in the field of wireless technology. These types of networks operate in the absence of fixed infrastructure, which makes them easy to deploy at any place and at any time [2], [4], and [7]. The absence of any fixed infrastructure in mobile ad-hoc networks makes it difficult to utilize the existing techniques for network services, and poses number of various challenges in the area. Typical

challenges include routing, bandwidth constraints, security and power.

Mobile ad-hoc networks are highly dynamic; topology changes and link breakage happen quite frequently. Therefore, we need a security solution, which is dynamic, too [6], [8] and [12]. Any malicious or misbehaving nodes can generate hostile attacks. These types of attacks can seriously damage basic aspects of security, such as integrity, confidentiality and privacy of the node. Current ad-hoc routing protocols are completely insecure. Moreover, existing secure routing mechanisms are either too expensive or have unrealistic requirements.

Security requirements for ad-hoc routing protocols includes:

- Certain discovery, meaning the route should always be found, if it exists between two nodes;
- Isolating misbehaving nodes, making sure misbehaving nodes should always be identified and isolated from routing; and
- Location privacy, protecting information about node location and network structure.

2. NEED OF SECURITY IN MANET

Security is one of the important aspects of this technology and it needs some serious attention. Users within the network want their communication to be secure. As current mobile ad-hoc networks do not have any strict security policy, this could possibly lead active attackers to easily exploit or possibly disable the mobile ad-hoc network. Security goals in mobile ad-hoc networks are reached through cryptographic mechanisms such as public key encryption or digital signature [13]. These mechanisms are backed by centralized key management where a trusted Certificate Authority (CA) provides public key certificate to mobile nodes in order to develop mutual trust between nodes. Any disturbance with the Certificate Authority can easily affect the security of the entire network [1].

2.1. Attacks in Ad-hoc Routing Protocols

An **active attack** injects arbitrary packets and tries to disrupt the operation of the protocol in order to limit the availability, gain authentication, or attract packets destined or other nodes.

A **passive attack** does not disrupt the operation of the protocol, but tries to discover valuable information by listening to traffic.

Incorrect traffic generation includes attacks which consist in sending false control messages i.e. control messages sent on behalf of another node (identity spoofing), or control messages which contain incorrect or outdated routing information. The consequences of this attack are degradation in network communications, unreachable nodes and possible routing loops[9].

Incorrect traffic relaying disrupts network communications coming from legitimate, protocol compliant nodes that are polluted by misbehaving nodes.

In conclusion, most of the proposed routing solutions are, as yet, incomplete when it comes to security issues[10], and [11]. We can trust a routing mechanism only when it guarantees that all transmission will be protected. Rather than treating these problems on individual basis, we'll need to work out routing along with security in mobile ad-hoc network designs going into the future.

2.3 Security Implementation Issues in MANETs

Securing wireless ad hoc networks is particularly difficult for many reasons including the following:

- **Vulnerability of channels.** As in any wireless network, messages can be eavesdropped and fake messages can be injected into the network without the difficulty of having physical access to network components.
- **Vulnerability of nodes.** Since the network nodes usually do not reside in physically protected places, such as locked rooms, they can more easily be captured and fall under the control of an attacker.
- **Absence of infrastructure.** Ad hoc networks are supposed to operate independently of any fixed infrastructure. This makes the classical security solutions based on certification authorities and on-line servers inapplicable.
- **Dynamically changing topology.** In mobile ad hoc networks, the permanent changes of topology require sophisticated routing protocols, the security of which is an additional challenge. A particular difficulty is that incorrect routing information can be generated by compromised nodes or as a result of some topology changes and it is hard to distinguish between the two cases.

3. AD HOC ON DEMAND DISTANCE VECTOR (AODV) ROUTING PROTOCOL

In AODV [3] nodes that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Further a node does not have to discover and maintain a route to another node until the two needs to communicate unless the former node is offering its services as an intermediate forwarding station to maintain

connectivity between two other nodes[5]. The algorithm's primary objectives are:

- To broadcast discovery packets only when necessary.
- To disseminate information about changes in local connectivity to those neighboring mobile nodes those are likely to need the information.

AODV is a combination of both DSDV (Destination sequenced distance vector) and DSR (Distance vector routing protocol), which can be explained as follows:

AODV uses a broadcast route discovery mechanism as is also used with modifications in the Dynamic Source Routing (DSR) algorithm. To maintain the most recent routing information between nodes the concept of destination sequence number from DSDV is borrowed. The combination of these techniques yields an algorithm that uses bandwidth efficiently by minimizing the network load for control and data traffic is responsive to changes in topology and ensures loop free routing.

Limitations

In fact we consider AODV as the default routing protocol as it is presently going to be the acceptable standard for ad hoc network. So, we will highlight the major attacks on AODV or major flaws of this protocol. It is to be noted that it is not hard to transform similar type of attacks on other protocols, DSR for example. Known attacks on AODV are as follows:

- Traffic redirection by modification
- Replay attacks
- Loop formation by spoofing
- False Route Error

Abu Raihan Mostofa Kamal [1] studied various types of existing routing protocols extensively with a view to finding security vulnerabilities. It is followed by highlighting major security attacks on Ad hoc On-demand Distance Vector (AODV) routing protocol which is on the verge of being the default routing standard for ad hoc network. Both the security requirement of applications and limitations of the mobile nodes have been carefully considered in order to design a feasible solution to counter possible attacks.

Manel Guerrero Zapata and N. Asokan [8] gave a solution of securing AODV termed as Secure AODV (SAODV). The basic principal of SAODV protocol depends on the authenticating most of the fields of the RREQ/RREP packets and the use of hash chain to authenticate hop count field.

In this work, authors proposes a solution which provides security for AODV routing protocol and study the relative performance of insecure AODV in ad-hoc networks. We used "Network Simulator" (version 2), developed at Berkley, to simulate the respective environment of ad-hoc network and then study the behavior of AODV protocol under different conditions.

4. SIMULATION RESULTS FOR NETWORK SIZE OF 5 NODES

In the following section, we have obtained results for AODV protocol keeping the network size of five nodes in terms of following parameters:

4.1 Throughput of Received Packets

After analyzing the graph below (Figure 1), we can conclude that AODV protocol performs fairly better when comes the case of throughput of received packets. During the whole transmission there is consistent reception of packets. Therefore, for a smaller number of nodes, both proactive and reactive protocols show same performance. But when our modified AODV protocol will be implemented then throughput may decrease due to process encryption and decryption that are used to provide security. So performance of AODV will be considerable but will provide security.

4.2 Packets Dropped

When number of dropped packets / TIL (Time Interval Length) was plotted against simulation time (Figure 2) following results were obtained: AODV performs better among the four routing protocols because packets are not sent until a route is not found. This is the major characteristic of a reactive routing protocol. But still packets are dropped due to absence of security. So when our proposed solution will be simulated packets dropped will be low.

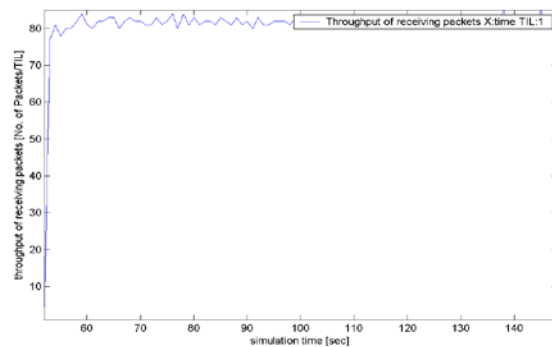


Fig 1: Throughput of receiving packets

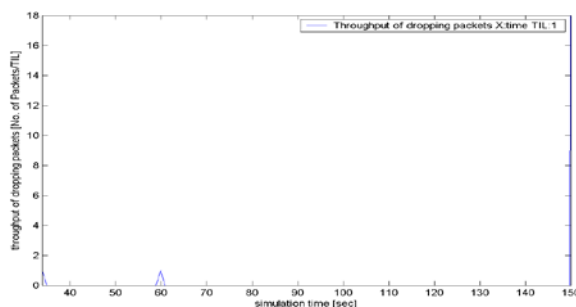


Fig 2: Throughput of Dropped Packets

4.3 End-to-End Delay

This parameter comprises all kind of delay i.e. delay that occurs when the packet is stored in a buffer before the node transmits it to other node, transmission delay etc. The results of simulation

are: In AODV route recovery is not very fast, therefore does not show a better delay performance than the other reactive protocols like DSR. It can be seen from graph (Figure 3).

But AODV with only HELLO messages has lowest delay on data packets that are received. The reason is that it finds route faster or that the routes that are shorter or more optimal, instead AODV with only Hello messages is the AODV version that gets significantly fewest packets through the network. The packets that it successfully gets through the network have approximately the same low delay as for other AODV versions. The difference is that other AODV versions have portion of packets that have higher delay. So the average delay becomes higher.

5. CONCLUSIONS

Our purpose of obtaining these simulation results is to analyze how AODV protocol performs in the absence of security in different network scenario. From the simulation results we have seen the performance of insecure AODV taking different parameters and network sizes. Our proposed methodology provides **secure routing** and **data transmission** for AODV and will provide satisfactory performance results in simulation environment.

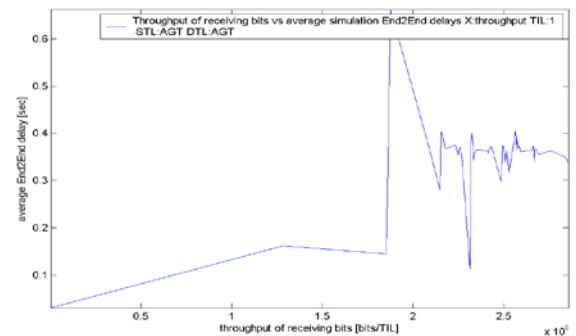


Fig 3: Throughput Vs delay

6. REFERENCES

- [1] A. Perrig, R. Canetti, J. D. Tygar, and D. X. Song, "Efficient authentication and signing of multicast streams over lossy channels", IEEE Symposium on Security and Privacy, 2000, pp 56-73.
- [2] A.S. Tenenbaum, "Computer Networks", 3rd Edition. Prentice Hall, 2000
- [3] Charles E. Perkins and Elizabeth M. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing", IETF, Internet draft, draft-ietf-manet-aodv-13.txt, 2003.
- [4] Elizabeth Royer and C-K Toh, "A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks", IEEE Personal Communications Magazine, April 1999, pp. 46-55.
- [5] George Coulouris, Jean Dollimore and Tim Kindberg "Distributed Systems Concepts and Design", 3rd Edition, Pearson Education, 2004, pp 251-289.
- [6] Josh Broch, David A. Maltz, David B. Johnson, et al. "A Performance Comparison of Multi-Hop Wireless Ad Hoc

- Network Routing Protocols”, MOBICOM’98, October 1998.
- [7] L. Zhou and Z.J. Haas, “Securing ad hoc networks,” IEEE Network, 0890-8044, November/December 1999, pp. 24-30.
 - [8] M. Guerrero Zapata and N. Asokan, “Securing Ad Hoc Routing Protocols”, Proc. ACM Workshop on Wireless Security (WiSe), ACM Press, 2002, pp. 1–10.
 - [9] Mike Burmester, Tri Van Le and Matt Weir, “Tracing Byzantine Faults In Ad Hoc Networks” ,Department of Computer Science, Florida State University, Tallahassee, Florida 32306, USA.
 - [10] N.Asokan and P. Ginzboorg, “Key agreement in adhoc networks”, Elsevier Science, Computer Communications 23, 0140-3664/00, PII:S0140- 3664(00)00249-8, 2000, pp.1627-1637.
 - [11] S. Marti et al. Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks. Proc. 6th Ann. Int’l Conf. Mobile Computing and Networking (MobiCom 2000), ACM Press, 2000, pp. 255–265.
 - [12] T. Clausen and P. Jacquet “Optimized Link State Routing Protocol (OLSR).” RFC 3626, IETF Network Working Group, October 2003.
 - [13] William Stallings, Cryptography and Network Security, 2nd Edition, 1999, Chapter 13, 403.