Middle-East Journal of Scientific Research 19 (9): 1199-1204, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.19.9.11216

# Wireless Networks Based on Aodv Routing Protocol

*P. Rachelin Sujae*

M.Tech Embedded Systems, Bharath University,
Assistant Professor, Chennai, India

**Abstract:** Security of wireless ad hoc network over insecure communication channel is a challenging task. In this paper, some of the threats to wireless ad hoc networks and specifically, some attacks against the AODV routing protocol are discussed. AODV tool is aimed at real-time detection of these attacks. The tool monitors network packets to detect local and distributed attacks within its radio range. In ad hoc networks, there is no established infrastructure or centralized administrator. Wireless ad hoc networks are vulnerable to various attacks. This paper surveys the various security issues and attacks possible in a wireless ad hoc network and motivates the need for an intrusion detection system. AODVSTAT is an intrusion detection tool that performs real-time detection of attacks in mobile ad hoc networks running the AODV routing protocol. Experimental results validate the ability of AODVSTAT to successfully detect both one-hop and distributed attacks against the AODV routing protocol, with a low number of false positives. Also, the tool imposes a small over- head on the network nodes, which is an important factor for resource-constrained equipment.

**Key words:** Wireless ad hoc network · Security · AODV routing protocol · Attacks · Intrusion detection system · MANET

## INTRODUCTION

Mobile ad hoc network (MANET) is a collection of mobile nodes that are capable of communicating with each other, establishing and maintaining connections as needed. In ad hoc networks, there is no established infrastructure or centralized administration. The topology of an ad hoc network is defined by the geographical positions and the transmission ranges of the nodes. These networks do not have a clearly defined physical boundary and, therefore, have no specific entry point. As a consequence, access control mechanisms, similar to firewalls in wired networks, are not feasible. In addition, the hop-by-hop routing used in ad hoc networks requires cooperation from the nodes in the network. Therefore, it is not possible to assume that the routing infrastructure can be trusted to any degree.

Wireless ad hoc networks are vulnerable to various attacks. These include passive eavesdropping, active interfering, impersonation and denial-of-service. Intrusion prevention measures, such as strong authentication and redundant transmission, can be used to address some of these attacks. However, these techniques can address only a subset of the threats and, moreover, are costly to implement.

The dynamic nature of ad hoc networks suggests that prevention techniques should be complemented by detection techniques that monitor the security status of the network and identify anomalous and/or malicious behavior. These techniques are usually less expensive to implement and can be easily deployed in existing ad hoc networks without requiring modifications to the nodes' configuration or the routing protocols being used. Intrusion detection techniques have traditionally been classified into two paradigms, namely anomaly detection and misuse detection [1]. Misuse detection can perform focused analysis of the audit data and usually produces very few false positives. However, it can detect only those attacks that have been modeled and possibly variations on those attacks. Anomaly detection has the advantage of being able to detect previously unknown attacks. This advantage is paid for in terms of the large number of false positives generated and the difficulty of training a system with respect to a highly dynamic environment.

**Corresponding Author:** P. Rachelin Sujae, M. Tech Embedded Systems, Bharath University, Chennai, India.

Previous work in intrusion detection for ad hoc wireless networks focused on identifying anomalous behavior patterns [2]. The primary concern with anomaly detection approaches is that the large number of false positives and the overhead involved in modeling the behavior of the system may be too expensive for mobile nodes [14-17].

Another limitation of previous intrusion detection approaches is that they have been validated using only simulation-based studies [2-5]. Simulations are typically useful when larger topologies are used for evaluation. However, simulation-based evaluations need to be complemented by implementation results, to completely understand the operational limits of the system and to evaluate the overhead.

This project describes AODVSTAT, a tool aimed at network-based, real-time intrusion detection for wireless networks based on the Ad hoc On-Demand Distance Vector routing protocol (AODV) [6]. The intrusion detection tool is based on a stateful misuse detection technique[7] that supports effective intrusion detection while keeping the number of false positives low. This tool has been evaluated through both simulation and implementation based testing [8-13].

This paper gives an overview of the AODV routing protocol and describes examples of possible attacks in an ad hoc wireless environment. It's also surveys previous work on securing ad hoc networks and presents the details of the attacks that were used to test the capabilities of AODVSTAT. It also discusses the results obtained in detecting attacks in wireless networks.

**Technique Adopted:** A mobile ad hoc network (MANET) is a collection of mobile nodes capable of communicating with each other, establishing and maintaining connections. In ad hoc networks, there is no established infrastructure or centralized administration. This paper has two major things. They are **D**etector (Sensor) and **C**ollection of **N**odes.

Any one acts as source or destination and also any one the remaining act as detector. Detector maintains a mesh table which has all nodes information. Detector is only given authentication for established communication between nodes.

The detector running gathers information about the ad hoc network by monitoring packets with in its radio range [18-22]. Hence, the sensor is able to detect attacks that are within its neighborhood. The sensor needs more than one-hop information to select most of the attacks. For instance, it can detect false message propagation attack only if it knows either the current sequence number of all the nodes in the network or the number of hops to all the nodes. The current version of AODVSTAT detects one –hop attack such as.

- **Spoofing**
- **Resource depletion**
- **Packet dropping attacks**

AODVSTAT extends the sequence control technique to detect MAC spoofing and uses stored mappings of MAC/IP pairs to detect IP spoofing attacks. When a packet arrives the MAC/IP information is stored for the first time. If another packet with the same IP but different MAC or vice versa, arrives, the packet is detected to be spoofed.

Packet dropping is detected by checking whether a sensor's neighbor forwards packets towards the final destination. Therefore, a neighbor table is maintained to determine the nodes that are neighbors of the Intrusion Detection System (IDS). A malicious node can deplete network resources by transmitting a large number of data or control packets. The IDS detects this by maintaining a count of the number of packets that it receives from each node within a specific time window. If this count crossed a threshold, then an alert is signaled.

**Log Files:** Log files are the files that are available in both Detector and Client node. These are like databases. Detector is actually taking the contents from log files and does their work based on this information. While detecting the system the detection tool getting information from the Client Log file and send that to the detector. After completing the work in that node the detector deletes the information stored in Client Log file [23-24].

**An Overview of Aodv Routing Protocol:** AODV [5], a tool aimed at network-based, real-time intrusion detection for wireless networks. When a source node needs a route to a destination, it initiates a route discovery process to locate the destination node.The source node S floods the network with a route request packet (RREQ), as shown in Fig 1, requesting a route to be set up to the destination D.

On receiving an RREQ, intermediate nodes update their routing table for a reverse route to the source. All the receiving nodes that do not have a route to the destination broadcast the RREQ packet to their neighbors, with an incremented hop count.

A route reply (RREP) is sent back to the source node when the RREQ query reaches either the destination itself or any other intermediate node that has a current route to

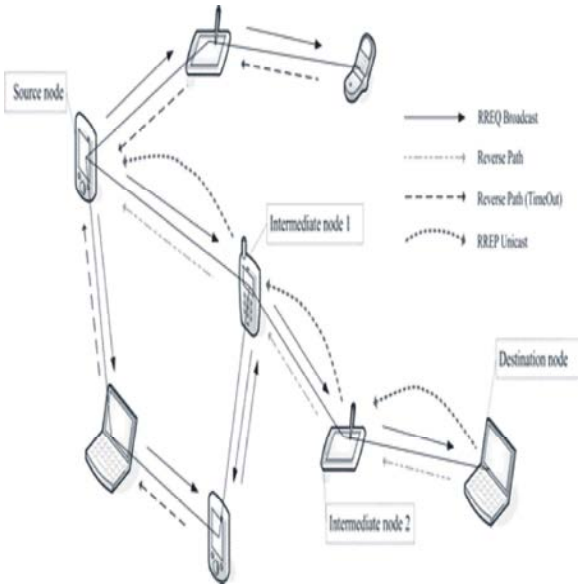



Fig. 1: Route Discovery Procedure of AODV Protocol

the destination. As the RREP propagates to the source, the forward route to the destination is updated by the intermediate nodes receiving an RREP packet. Both the destination node D and intermediate node G have a route to the destination.

Hence, they reply to the RREQ with an RREP packet. AODV uses sequence numbers to determine the freshness of routing information and to guarantee loop-free routes.

In case of multiple routes, a node selects the route with the highest sequence number. If multiple routes have the same sequence number, then the node picks the route with the shortest hop-count. Timers are used to keep the route entries fresh. When a link break occurs, route error (RERR) packets are propagated along the reverse path to the source, invalidating all broken entries in the routing tables of the intermediate nodes. AODV also uses periodic HELLO messages to maintain updated information about the connectivity of neighboring nodes.

The AODV protocol does not incorporate any specific security mechanism, such as strong authentication. Therefore, there is no obvious way to prevent mischievous behavior such as MAC spoofing, IP spoofing, dropping packets, or altering the contents of control packets. Protocols like SAR and SAODV protect AODV against a limited number of attacks but at the cost of performance in terms of overhead and latency [25-27].

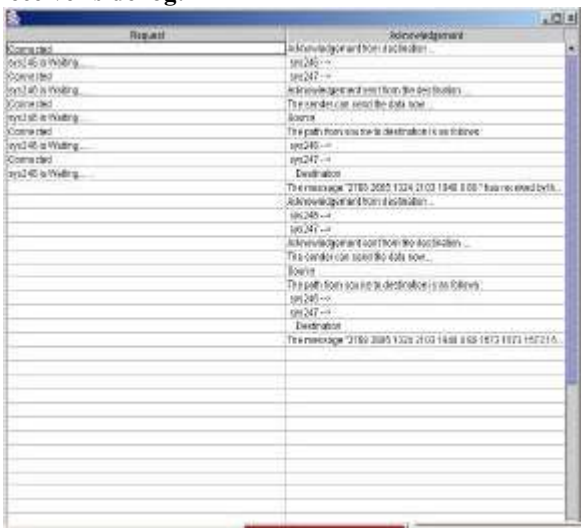
**Design Implementation:** Several procedures developed to satisfy the request of the mobile node communication and also its security.

- To run the detector in order to monitor nodes and also to discover the shortest path for communication between source node and destination node
- Detector maintain log file for nodes information such as name of the node and its ip address. It will store in mesh table.
- Checking process for validation in the detector.
- Registration process in the detector to add or remove the node.
- In order to open the application after detector validation.
- Some numerical value is assigned to set the Threshold level for dropping of packet.

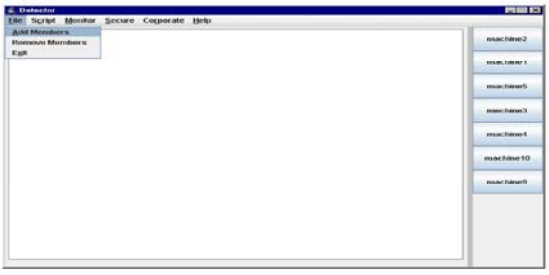
## RESULTS

**Form Design:**

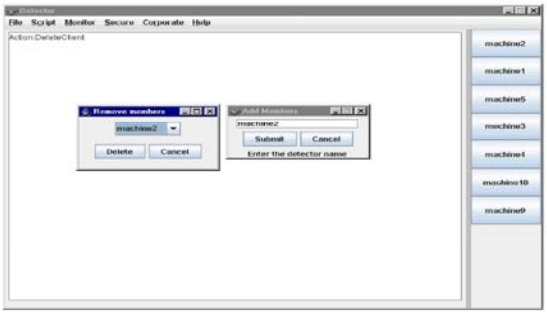

**Receiver side log:**



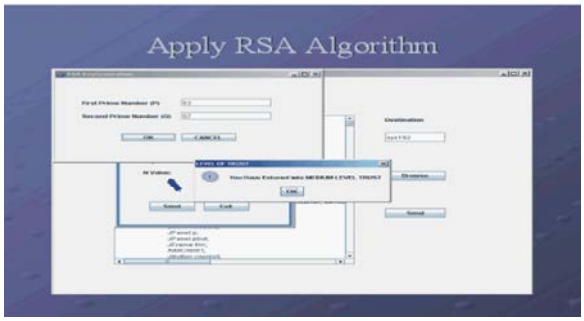

**Detector:**



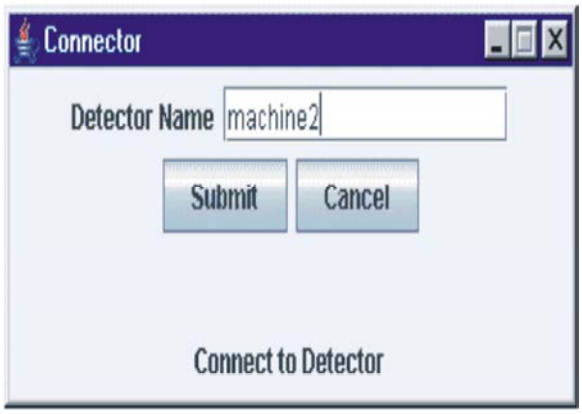
**Detector Add or remove members:**



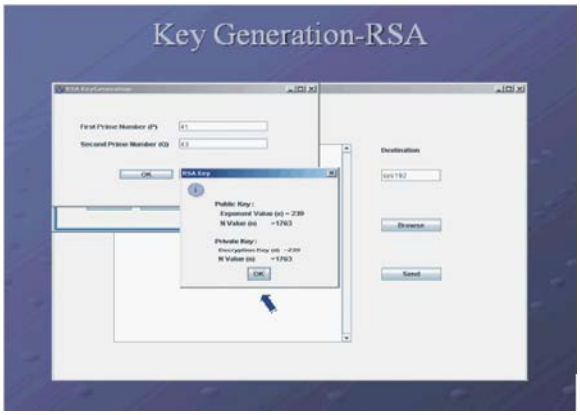

**RSA Algorithm:**



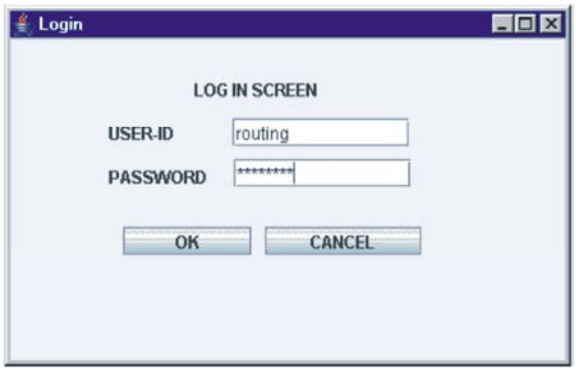

**Single node:**



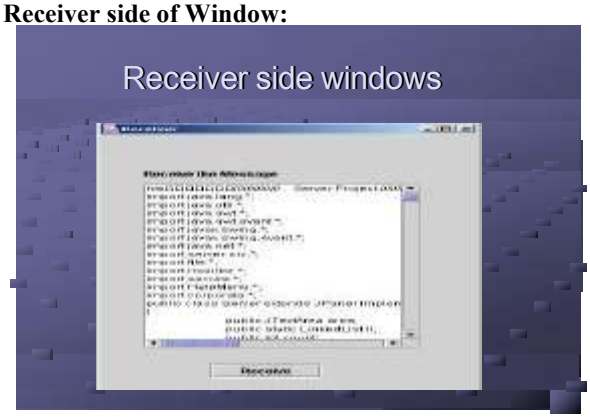

**Key Generation of RSA:**




**Node Login:**

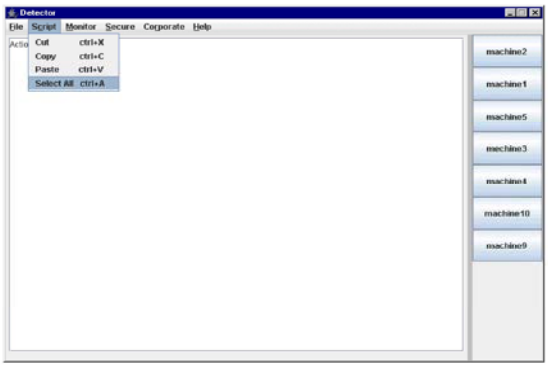



**Receiver side of Window:**

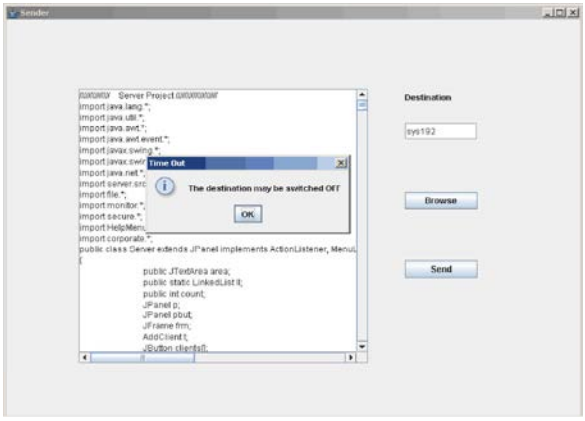



**Node Application Window:**

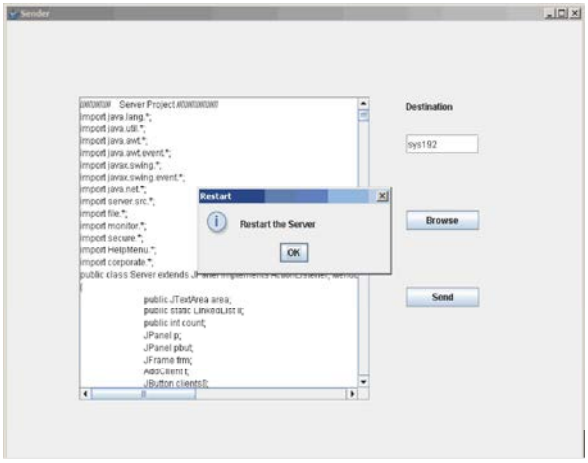
**Script Detector:**



**Destination:**




**Restart the window:**




## CONCLUSION

This project surveys the various security issues and attacks possible in a wireless ad hoc network and motivates the need for an intrusion detection system. AODVSTAT is an intrusion detection tool that performs real-time detection of attacks in mobile ad hoc networks running the AODV routing protocol. Experimental results validate the ability of AODVSTAT to successfully detect both one-hop and distributed attacks against the AODV routing protocol, with a low number of false positives. Also, the tool imposes a small over- head on the network nodes, which is an important factor for resource-constrained equipment.

## REFERENCES

1. Debar, H., M. Dacier and A. Wespi, 1999. Towards a taxonomy of intrusion-detection systems. Computer Networks, 31(8): 805-822.
2. Zhang, Y. and W. Lee, 2000. Intrusion Detection in Wireless Ad-hoc Networks. In Proceedings of the International Conference on Mobile Computing and Networking, pp: 275-283, Boston, MA.
3. Marti, S., T.J. Giuli, K. Lai and M. Baker., 2000. Mitigating Rout- ing Misbehavior in Mobile Ad hoc Networks. In Proceedings of the International Conference on Mobile Computing and Networking, pp: 255-265, Boston, MA.
4. Stamouli, I., 2003. Real-time intrusion detection for ad hoc net- works. Master's thesis, University of Dublin.
5. Perkins, C.E. and E.M. Royer, 1999. Ad-hoc On-Demand Distance Vector Routing. In Proceedings of the IEEE Workshop on Mobile Computing Systems and Applications, pp: 90-100, New Orleans, LA.
6. Vigna, G., F. Valeur and R. Kemmerer, 2003. Designing and Implementing a Family of Intrusion Detection Systems. In Proceedings of the European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of SoftwareEngineering (ESEC/FSE 2003), Helsinki, Finland.
7. Albers, P., O. Camp, J.M. Percher, B. Jouga, L. Me and R. Puttini, 2002. Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches.In The International Workshop on Wireless Information Systems, Proceedings of the International Conference on, Proceedings of the Enterprise Information Systems, Ciudad Real, Spain.
8. Bellardo, J. and J. Savage., 2003. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions. In Proceedings of the USENIX Security Symposium, Washington DC.
9. Buchegger, S. and J.Y.L. Boudec, 2002. Performance Analysis of the CONFIDANT Protocol. In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing, pp: 226-236.
10. Chakeres, I.D., XXXX. AODV-UCSB Implem'n from University of California Santa Barabara. http:// moment.cs.ucsb.edu/ AODV/aodv.html.
11. Hu, Y.C., D.B. Johnson and A. Perrig, 2002. Ariadne: A Secure On-Demand Routing Protocol for Ad hoc Networks. In Pro- ceedings of the ACM International Conference on Mo bile Computing and Networking (Mobicom), Atlanta, GA.
12. Hu, Y.C., D.B. Johnson and A. Perrig, 2002. Sead: Secure efficient

13. Distance vector routing in mobile wireless ad hoc networks. In Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA ' 02), pp: 3-13.
14. Ilgun, K.R., A. Kemmerer and P.A. Porras, 1995. State Transition Analysis: A Rule-Based Intrusion Detection Approach. IEEE Transactions on Software Engineering, 21(3): 181-199.
15. Kong, J., P. Zerfos, H. Luo, S. Lu and L. Zhang, 2001. Provid- ing Robust and Ubiquitous Security Support for Mobile Ad Hoc Networks. In Proceedings of the IEEE Internationa Conference on Network Protocols, Riverside, CA.
16. Mishra, A. and W. Arbaugh, 2002. An Initial Security Analysis of the IEEE 802.1X Protocol. Technical Report, Department of Computer Science, University of Maryland, February. Sanzgiri, K., B. Dahill, B.N. Levine, C. Shields and E. Belding-Royer, 2002. A Secure Protocol for Ad Hoc Networks. In
17. Vigna, G., F. Valeur and R. Kemmerer, 2003. Designing and Implementing a Family of Intrusion Detection Systems. In Proceedings of the European Software Engineering Conference and ACM SIGSOFT Symposium on the Foundations of SoftwareEngineering (ESEC/FSE 2003), Helsinki, Finland.
18. Wright, J., 2003. Detecting Wireless LAN MAC Address Spoofi ng. White Paper.
19. Naldurg, S. Yi, P. and R. Kravets, 2001. Security Aware Ad Hoc Routing for Wireless Networks. In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Com- puting, Poster Session, pages 299-302, Long Beach, Califor- nia.
20. Chun, H. Yih- and A. Perrig, 2004. A survey of secure wireless ad hoc routing. IEEE Security & Privacy Magazine, 2(3): 28-39.
21. Zapata, M.G. and N. Asokan, 2002. Securing Ad-Hoc Routing Pro- tocols. In Proceedings of the 2002 ACM Workshop on Wire- less Security, pp: 1-10, Atlanta, GA.
22. Zhang, Y. and W. Lee, 2000. Intrusion Detection in Wireless Ad-hoc Networks. In Proceedings of the International Conference on Mobile Computing and Networking, pp: 275-283, Boston, MA.
23. Zha, Y. and W. Li An integrated environment for testing mobile ad-hoc networks. In Proceedings of the Third ACM International Symposium on Mobile Ad Hoc Network- ing and Computing, (MobiHo ' 02), Lausanne, Switzerland.
24. Zhou, L. and Z.J. Haas, 1999. Securing AdHoc Networks. IEEE Network Magazine, 13(6): 24-30.
25. Tatyana Aleksandrovna Skalozubova and Valentina Olegovna, 2013. Reshetova Leaves of Common Nettle (Urtica dioica L.) As a Source of Ascorbic Acid (Vitamin C), World Applied Sciences Journal, 28(2): 250-253.
26. Rassoulinejad-Mousavi, S.M., M. Jamil and M. Layeghi, 2013. Experimental Study of a Combined Three Bucket H-Rotor with Savonius Wind Turbine, World Applied Sciences Journal, 28(2): 205-211.
27. Vladimir G. Andronov, 2013. Approximation of Physical Models of Space Scanner Systems World Applied Sciences Journal, 28(4): 528-531.