Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.224 – 230

RESEARCH ARTICLE

Protecting Mobile Ad Hoc Networks from Black Hole Attacks

MARPU DEVADAS[1], K. VINAY KUMAR[2]

[1]Department of CSE, Gokul Institute of Technology and Sciences, Piridi village
Bobbili mandalam ,Vizianagaram dt. Jntu kakinada university A.P, India
[2]Assistant Professor, Department of CSE, Gokul Institute of Technology and Sciences, Piridi village
Bobbili mandalam ,Vizianagaram dt. Jntu kakinada university A.P, India
[1] marpudevadas@gmail.com, [2] vinaykumar.gokul0@gmail.com

Abstract- Mobile Ad Hoc Network (MANET) is a communication that network that is made up of nodes that are self configured without having the need for fixed infrastructure. The nodes are vulnerable to various kinds of attacks due to their mobility and resource constrained nature. One such attack is black hole attack. In this attack a compromised node advertises itself to have a shortest path for sending data packets to destination. This way the malicious node deceives other nodes and obtains sensitive information. In this paper we proposed an authentication mechanism based on the solution provided recently by Luo et al. We built a prototype system that simulates the black hole attacks on MANET and the prevention measures. The prototype demonstrates the proof of concept pertaining to protecting MANET from black hole attacks. The simulation results are encouraging.

Index Terms – Mobile Ad Hoc Network, black hole attack, authentication, security

I. INTRODUCTOIN

Mobile Ad Hoc Networks are widely used for communications in case of emergencies and rescue operations in both civilian and military pursuits. The nodes in MANET can act as both transmitter and receiver. The transmitter takes care of sending data to other node while the other node can act as receiver and transmitter in order to forward the packets to destination. The source node S sends data to destination D which is not in the transmission range of D. In this case, the S sends data to nearby node that is supposed to forward packets to the other node in the path to destination. Thus the nodes in MANET are supposed to act as both transmitter and receiver. Figure 1 shows sample MANET.

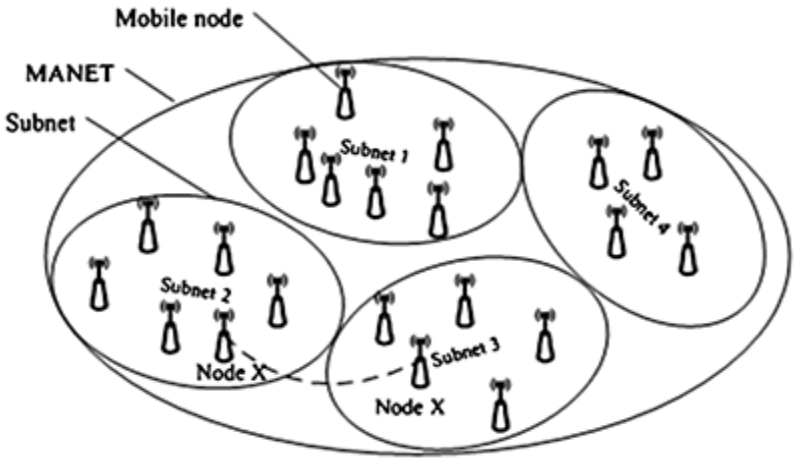

Figure 1 – Sample MANET

As can be seen in Figure 1, the nodes in MANET are part of the network and there might be sub networks within a big MANET. The nodes in MANET are vulnerable to attacks such as black hole attack. Such attack can jeopardize the interests of the purpose of the network.

In this paper we prevent such attacks in MANET by proposed effective security mechanism such as authentication which can avoid communication from malicious nodes. The security goals include confidentiality, availability, authentication, integrity, assurance, and non-repudiation. The proposed simulation is made using Java programming language. Java SWING API is used to provide intuitive user interface. The remainder of the paper is structured as follows. Section II provides review of literature. Section II reviews literature on prior works. Section III presents the proposed methodology. Section IV provides implementation and results. Section V concludes the paper besides providing directions for future work.

II. RELATED WORKS

This section provides the insights gained from review of literature. The important insights obtained from the literature [1]-[10] are as given below.

- Black hole attacks are one of the kinds of attacks that are possible on MANET. The black hole attacks make MANETs vulnerable as they can exploit to gain sensitive information from MANET devices.
- AODV protocol used in MANET has many issues. It is vulnerable to attacks such as Rush Attack, False message propagation attack, false reply attack, and black hole attack.
- Encryption and decryption are the widely used techniques for securing communications in communication networks.
- Important security requirements of any network include non-repudiation, assurance, integrity, authentication, availability and confidentiality.
- The black hole attack attracts MANET nodes to respond to the claims of malicious node and route packets through malicious node to facilitate it to gain access to unauthorized data.
- Authentication is one of the mechanisms that can be used to prevent black hole attacks. This process needs other support mechanism in order to have fool proof security in MANETs.

III. PROTOTYPE APPLICATION

We built a prototype application that simulates the proof of concept of a network application that mimics MANET and demonstrates the black hole attacks and the prevention mechanisms. The environment used to build the application is a PC with 4 GB RAM, core 2 dual processor running Windows 7 operating system. Figure 2 presents the user interface and mechanisms required by a sender node in MANET.

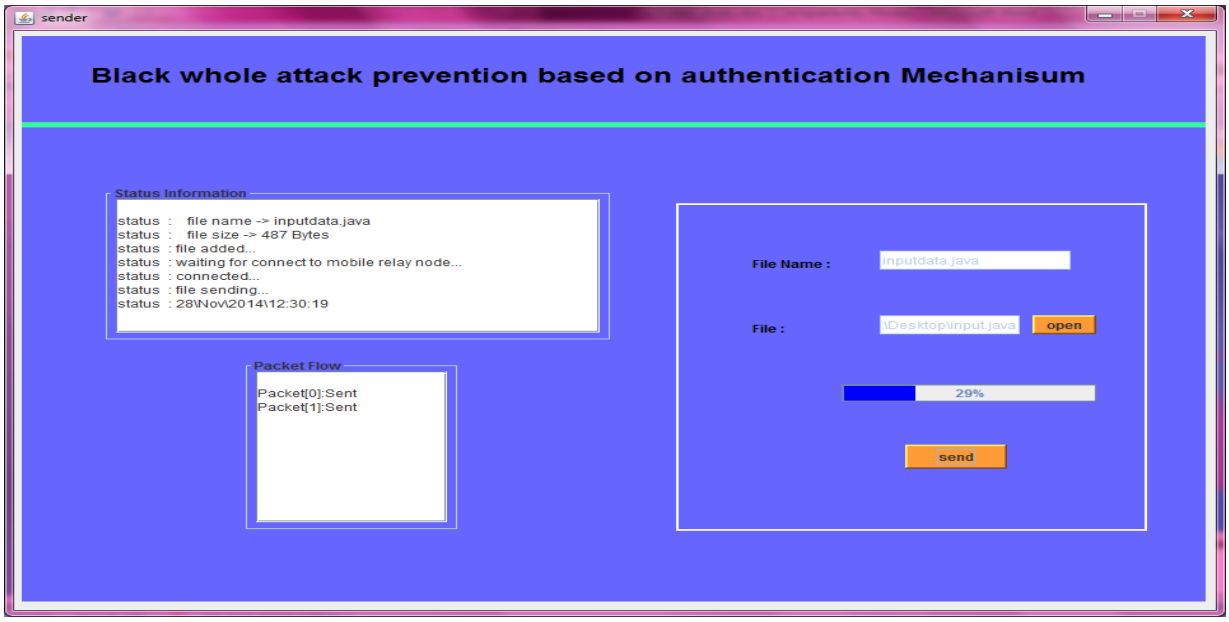

Figure 2 – Simulates sender node in MANET

As can be seen in Figure 2, it is evident that the sender node is able to send information to other node. The status of the data being flown and the packet flow are presented in the UI.

Figure 3 – Simulates receiver node in MANET

As can be seen in Figure 3, it is evident that the receiver node is able to receive information from other node. The status information is presented in UI besides having provision for downloading files, deleting them and viewing all files.

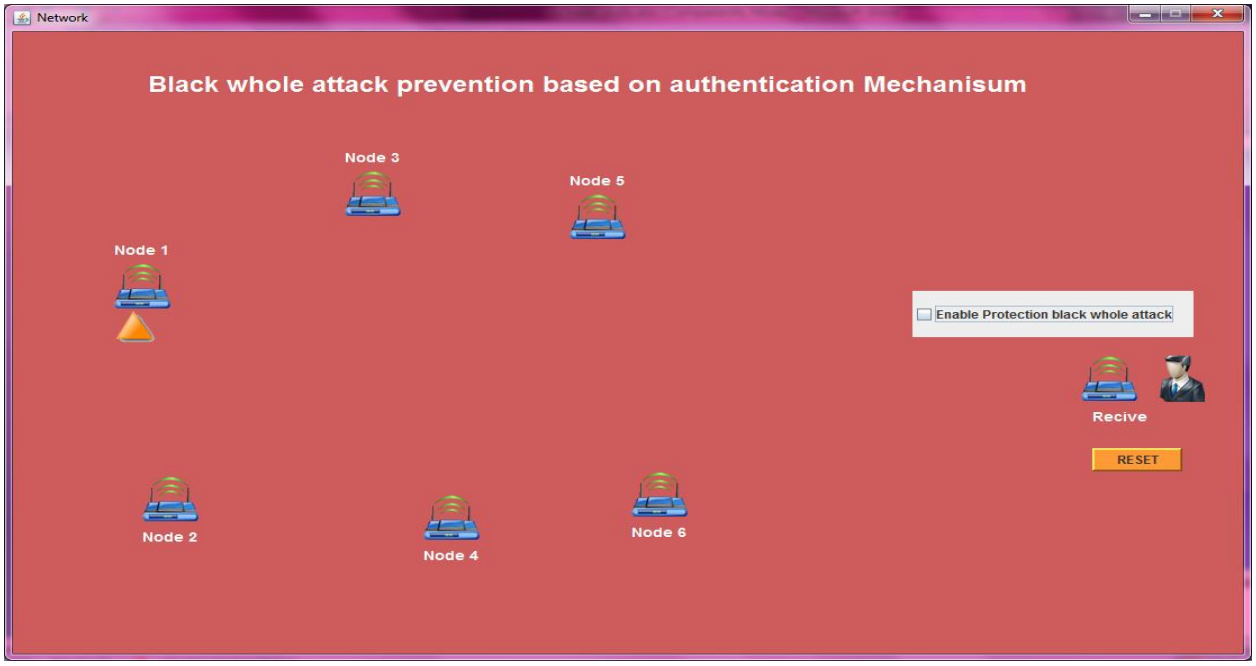

Figure 4 – Network simulation UI

As can be seen in Figure 4, it is evident that the MANET is simulated with six nodes. There is provision for running it without having prevention to black hole attack and with provision to prevent the attack.

IV. SIMULATION RESULTS

Simulations are made with two protocols namely AM and AODV with respect to simulation time and overhead; number of black hole nodes and data packet delivery ratio; false negative probability and simulation time; simulation time and detection time.

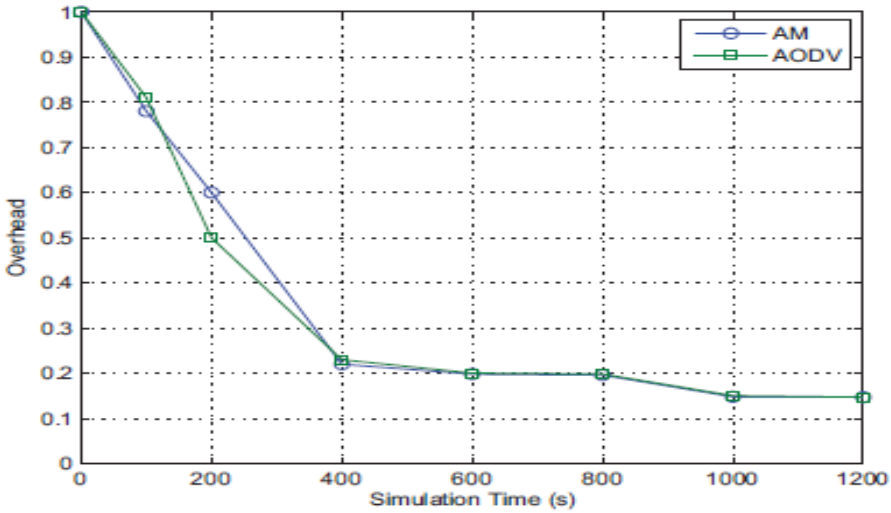

Figure 5 – Control overhead

As can be seen in Figure 5, it is evident that there is performance comparison between AM and AODV in terms of simulation time and overhead. It appears that AM has more overhead when compared with AODV.

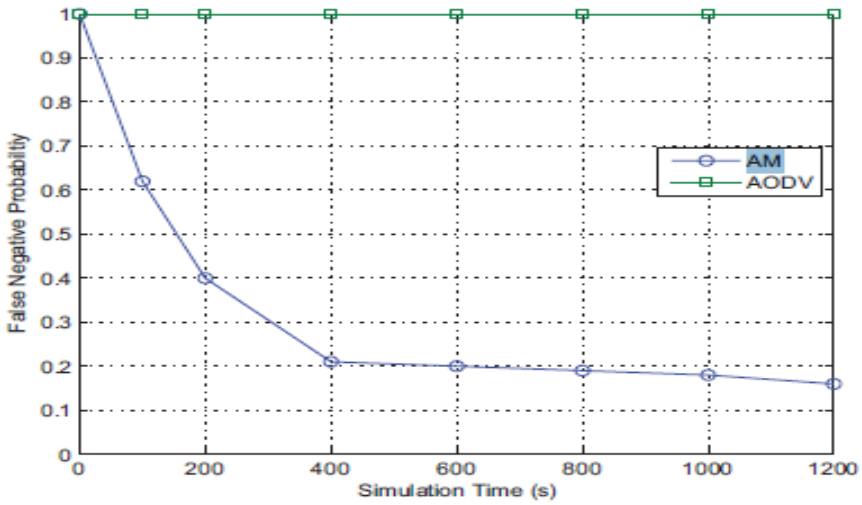

Figure 6 – False negative probability

As can be seen in Figure 6, it is evident that there is performance comparison between AM and AODV in terms of simulation time and false negative probability. It appears that AM has less false negative probability when compared with AODV.

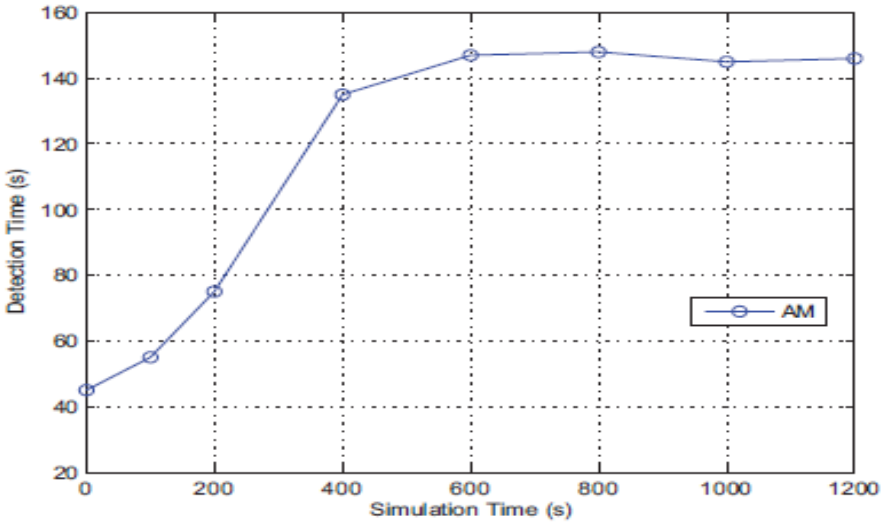

Figure 7 – Detection time

As can be seen in Figure 7, it is evident that there is performance AM shown with respect to detection time. It appeared that detection time is more as simulation time increases.

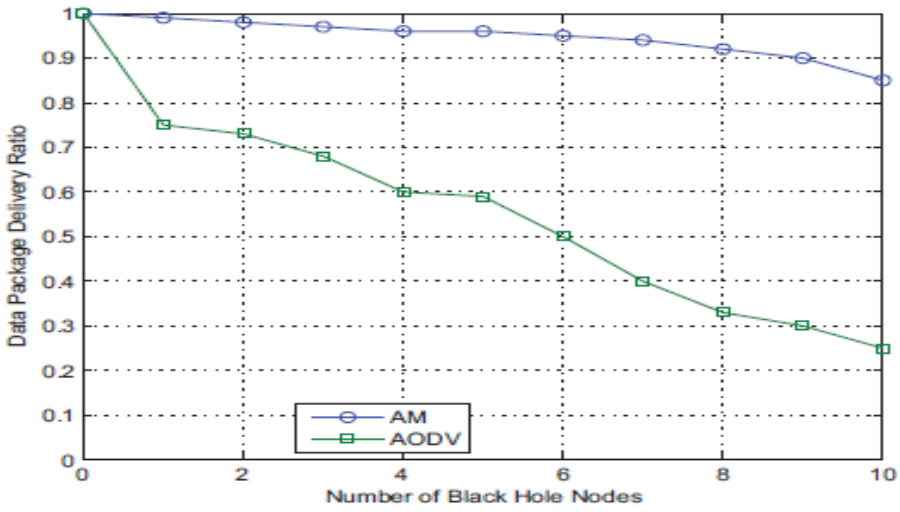

Figure 8 – Data packet delivery ratio

As can be seen in Figure 8, it is evident that there is performance comparison between AM and AODV in terms of number of black hole nodes and data delivery ratio. It appears that AM has more data delivery ratio when compared with AODV.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we studied various kinds of attacks made on MANET. Especially we focused on black hole attack which causes the nodes to expose sensitive information to adversaries. Black hole attack is an attack where a malicious node broadcasts a message saying that through it other nodes can find shortest path. For this reason other nodes believe that and use the malicious node's claim to send packets through that root believing that as shortest path. This is exploited by malicious node and gets the sensitive information being exchanged among the nodes. This kind of attack is named as black hole attack. We proposed an authentication mechanism that can prevent this attack in MANET. We built a prototype MANET system that simulates the proof of concept. The simulation results revealed that the proposed solution is able to prevent black hole attacks in MANET. One future direction is to implement the solution in real MANET devices and test the effectiveness of our solution.

REFERENCES

[1] Y.-C. Hu, D. B. Johnson, and A. Perrig, "Sead: Secure efficient bdistance vector routing for mobile wireless ad-hoc networks," in WMCSA '02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications. Washington, DC, USA: IEEE Computer Society, 2002, pp. 3–13.
[2] X. Wang, T. liang Lin, and J. Wong, Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network. Technical Report, Computer Science, Iowa State University, 2005.
[3] J. Grønkvist, A. Hansson, and M. Skøld, Evaluation of a Specification-Based Intrusion Detection System for AODV. di.ionio.gr/medhocnet07/wp-content/uploads/papers/90.pdf, 2007.
[4] S. Kurosawa, H. Nakayama, and N. Kato, "Detecting black hole attack on aodv based mobile ad-hoc networks by dynamic learning method," International Journal of Network Security, pp. 338–346, 2007.
[5] K. Makki, N. Pissinou, and H. Huang, "Solutions to the black hole problem in mobile ad-hoc network," 5th World Wireless Congress, pp. 508–512, 2004.
[6] M.-C. Basile, M.-Z. Kalbarczyk, and F.-R. K. Iyer, "Inner-circle consistency for wireless ad-hoc networks," IEEE Transactions on Mobile Computing, vol. 6, no. 1, pp. 39–55, 2007.
[7] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputationbased incentive scheme for ad-hoc networks," Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE, vol. 2, pp. 825–830, 21-25 March 2004.
[8] Y.-R. Tsai and S.-J. Wang, "Two-tier authentication for cluster and individual sets in mobile ad-hoc networks," Comput. Netw., vol. 51, no. 3, pp. 883–900, 2007.

[9] S. Sreepathi, V. Venigalla, and A. Lal, A Survey Paper on Security Issues Pertaining to Ad-Hoc Networks. www4.ncsu.edu/ sssreepa/Adhoc-networks-Security-Survey.doc.
[10] Y.-R. Tsai and S.-J. Wang, "Routing security and authentication mechanism for mobile ad-hoc networks," Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th, vol. 7, pp. 4716–4720 Vol. 7, 26-29 Sept. 2004.
[11] C. Basile, Z. Kalbarczyk, and R. Iyer, "Neutralization of errors and attacks in wireless ad-hoc networks," Dependable Systems and Networks, 2005. DSN 2005. Proceedings. International Conference on, pp. 518–527, 28 June-1 July 2005.
[12] L. Junhai, X. Liu, and Y. Danxia, "Research on multicast routing protocols for mobile ad-hoc networks," Comput. Netw., vol. 52, no. 5, pp. 988–997, 2008.
[13] A. Patcha and A. Mishra, "Collaborative security architecture for black hole attack prevention in mobile ad-hoc networks," Radio and Wireless Conference, 2003. RAWCON '03. Proceedings, pp. 75–78, 10-13 Aug. 2003.
[14] B. Sun, Y. Guan, J. Chen, and U. Pooch, "Detecting black hole attack in mobile ad-hoc networks," Personal Mobile Communications Conference, 2003. 5th European (Conf. Publ. No. 492), pp. 490–495, 22-25 April 2003.

AUTHORS

MARPU DEVADAS is currently working towards his M.Tech degree in Gokul Institute of Technology and Sciences, Piridi village, Bobbili mandalam ,Vizianagaram dt, A.P, India. His research interests include Networking and cloud computing

K. Vinay Kumar is working as an Assistant professor Gokul Institute of Technology and Sciences, Piridi village, Bobbili mandalam ,Vizianagaram dt, A.P,India. His main research interests are data mining and big data mining.

