Robust Defense Scheme against Selective Drop Attack in Wireless Ad-hoc Networks

Manjunatha P V[1], Machupalli Swetha Reddy[2], Anusha K[3], Marineni Sreenivasulu[4], Dadimi Vivekananda Reddy[5]

[1] Faculty in Department of Computer Science Engineering, S J C Institute of Technology, Chikkaballapur, India
[2,3,4,5] Department of Computer Science Engineering, S J C Institute of Technology, Chikkaballapur, India

---***---

Abstract: Detecting packet drop attacks is important for security of MANETs and current random audit based mechanism cannot detect collaborative attacks. In this we design a hash function bash method to generated node behavioral proofs that contain information from both data traffic and forwarding paths. The new method is robust against collaborative attacks described in the paper and it introduces limited computational overhead on the intermediate nodes. We investigate the security of the proposed approach and design schemes to further reduce the overhead.

Keywords: MANET,

1. INTRODUCTION

MANET (Mobile Ad-hoc Network) is a packet-based wireless network inclusive of mobile nodes group in which communication and movement will be at equivalent time, with no usage of fixed wired infrastructure. MANET is combination of self-organizing and adaptive networks which forms and deforms between themselves with no actual necessity of centralized administration. Otherwise, MANET is a sort of unplanned network where change of locations and configurationwill happen during the process without stopping the motion/process. Because MANETS use wireless connections to link to diverse networks. this can be a typical Wi-Fi connection or like a satellite transmission.

MANET's as the capability of multi-hop routing. The security, routing and host configuration metby distribution administration. In MANET nodes can leave and join the network at any movementMobile nodes are created with light weight, low memory and less power features. This comparatively the efficiency, reliability, stability and scope of wireless links are a thigh range to wired networks. All the nodes in the Network must have look alike features with identical capabilities and responsibilities which results

2. LITERATURE SURYEY

I. Routing security in wireless ad-hoc networks, Author: H. Deng, W. Li, and D.P. Agrawal, **Year:** 2002.

In thisarticle a mobile ad hoc network consists of a collection of wireless mobile nodes that are capable of communicating with each other without the use of a network infrastructure or any centralized administration. MANET is an emerging research area with practical applications. However, wireless MANET is particularly vulnerable due to its fundamental characteristics, such as open medium, dynamic topology, distributed cooperation, and constrained capability Routing plays animportant role in the security of the entire network. In general, routing security in wireless MANETS appears to be a problem that is not trivia to solve. In this article we study the routing security issues of MANETS, and analyze in detail one type of attack-the "black hole" problem- that can easily be employed against the MANETS. We also propose a solution for the black hole problem for ad hoc on-demand distance vector routing protocol.

II Trust threshold based public key management mobile ad hoc networks, Author: H. Cho, R. Chen, and K. S. Chan, **Year**: 2016.

In this article a packet has to be delivered within a distinct time limit as data delivery is a critical issue in a wireless network. In emergency situations, real-time data distribution of multimedia file is addressed using wireless network. The real-time data examined here are image and audio files and these files are broken into sequence of packets and forwarded tothe destination peer node based on a Priority algorithm.

Prioritized data dissemination processes the sequence of packets to be forwarded based on permanent priority scheduling. The packets areencrypted based on Trust based Public key management using public key generated in key generation phase and decrypted at the receiver end.

I. Routing security scheme based on reputation evaluation in hierarchical ad hoc networks, Author: Y. Yu, L. Guo, X. Wang, and C.Liu, **Year**: 2010.

In this paper, we propose a new RoutingSecurity Scheme based on Reputation Evaluation (RSSRE) to meet security requirements inhierarchical ad hoc networks. In this model, the reputation relationship is defined in considerationof the related node roles and functions, while the reputation evaluation mechanism is built based on the correlation among nodes that need to be evaluated. The dynamic reputation threshold is usedto improve routing security with the precondition of usability. The reputation information of nodesis updated with different roles. We can reconstruct the route to solve attack problems in transmitting packets. Simulation results show that compared with traditional reputation evaluationmodels, the proposed model in this paper can more timely and accurately reflect security status and execute improved routing when there are malicious nodes in hierarchical Ad Hoc networks.

II. Detecting unauthorized and compromised nodes in mobile ad hoc networks, AdHoc Netw., Author: N. Komninos, D. Vergados, and C. Douligeris, **Year**: 2007.

Security of mobile ad hocnetworks (MANET) has become a more sophisticated problem than security in other networks, due to the open nature and the lack of infrastructure of such networks. In this paper, the security challenges in intrusion detection and authentication are identified and the different types of attacks are discussed. We propose a two-phase detection procedure of nodes that are not authorized for specific services and nodes that have been compromised during their operation in MANET. The detection framework is enabled with the main operations of ad hoc networking, which are found at the link and network layers. The proposed framework is based on zero knowledge techniques, which are presented through proofs.

I. An accurate and precise malicious node exclusion mechanism for ad hoc: Networks," Ad hocNetw.,M. B. Duarte, **Year**:2014.

Mobile ad hoc networks are attractive due to the wireless communication, infrastructure-less design and the self-organized mobile nodes. These features, however, introduce vulnerabilities, since there are no centralized control elements and the communication depends on cooperation of nodes. We propose a robust and distributed access control mechanism based on a trust model to secure the network and stimulate cooperation by excluding misbehaving nodes from the network. The mechanism divides the access control responsibility into two contexts: local and global. The local context responsibility is the neighborhood watch to notify the global context about suspicious behavior. In its turn, the global context analyzes the received information and decides whether it punishes the suspicious node using a voting scheme. We model the exclusion mechanism and perform a parameter analysis. Simulation results prove that the combination of voting and trust schemes provides an accurate and precise classification and node exclusion mechanism, even though in scenarios of limited monitoring.

3. METHODOLOGY

a. The software sends packets with increasing size and it's provides the time taken to transferthe block and throughput in bits/sec, number of bits in the block transfer the information.

b. The Knowledge behind collective the packet size is to compare and measure the throughput for various packets sizes. Ideally, for small packet size, the throughput is less and with increasing packet size, it increases until a point after which is saturates.

4. Proposed System

- DSR may be a loop-free, on-request (reactive) routing protocol that relies upon source routing.
- It is a self-organizing and self-

configuring method.

There are three phases of DSR protocol: -

i. Route Discovery

ii. Route cache

iii. Route Maintenance

4.1 Advantages

- The major key advantages of this project are:
- In this Networks security ensures the integrity, availability, and performance ofWANETs.
- It helps to prevent critical service interruptions.
- Increases economic productivity by keeping network functioning properly.

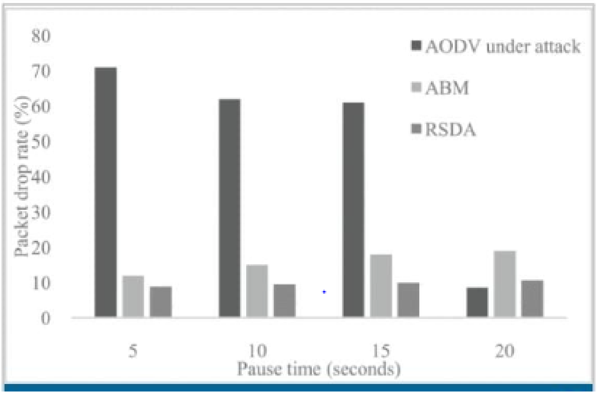
4.2 Objectives

- Resistive to select drop attack acts as security for drop attack and it's important thatnodes should know which overload a host and isolate a network.
- The selective drop attack actually will not forward message to next node but now it's forwarding messages due to malicious nodes. As a malicious nodes have to detect which is overloading a host and stop it from working.

5. Results

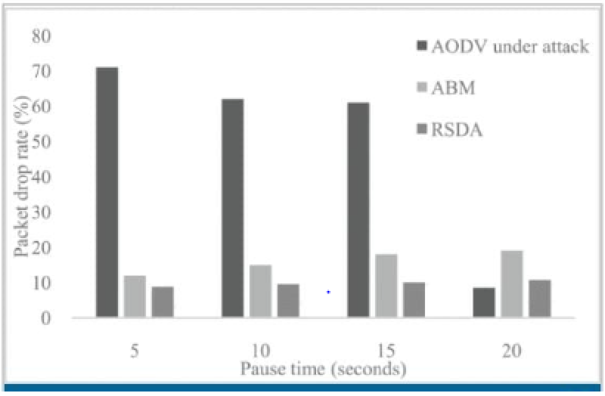
A. Packet Drop Rate

The drop rate was raised to about 63.9% when there were gray hole nodes randomly fixed at various positions at all pause time as 5, 10, 15,20 seconds respectively. In the presence of gray hole nodes, the total packet drop rate of the approach achieved was16.7%. With the deployment of proposed RSDA, the drop rate successfully reduced to about 9.56% rate The packet drop rate is shown to decrease significantly when more misbehaving nodes make abnormal routing operations.



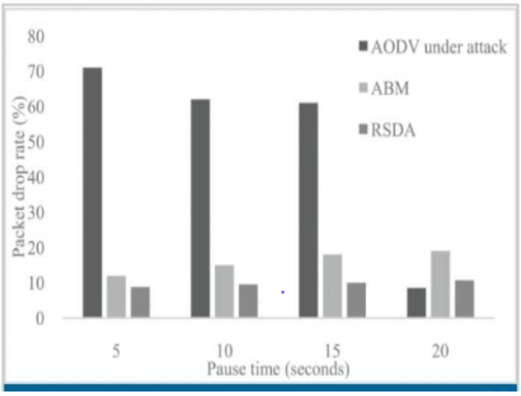
B. Jitter

Jitter value raised to about 0.56% when there were gray hole nodes randomly fixed at various positions at all pause time as 5s, 10s, 15s, 20seconds respectively. As presented in figure 10, in the presence of gray hole nodes, the total delay of the approach achieved was 0.14%. With the deployment of proposed RSDA, the jitter rate was successfully reduced to about 0.115% rate.



C. Routing Overhead

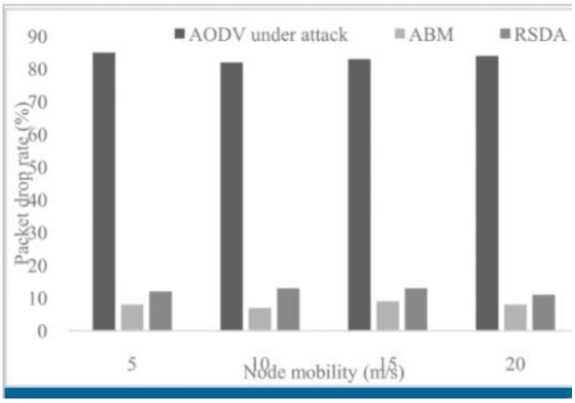
The routing overhead was raised to about 77.84% when gray hole nodes were randomly fixed at various positions at all pause time as 5s, 10s, 15s, 20seconds respectively. In the presence of gray hole nodes, the routing overhead of the existing approach was56.85%. With the deployment of proposed RSDA, the routing overhead was successfully reduced to about 45.49% rate

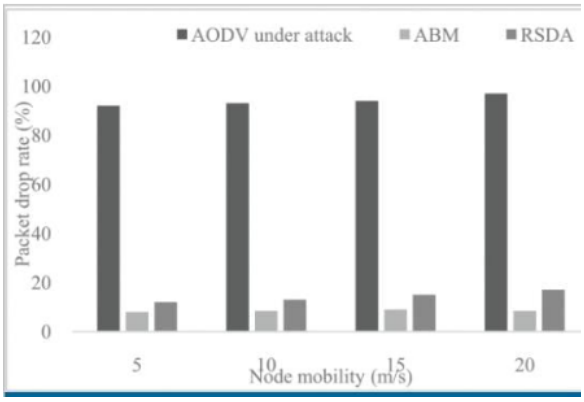


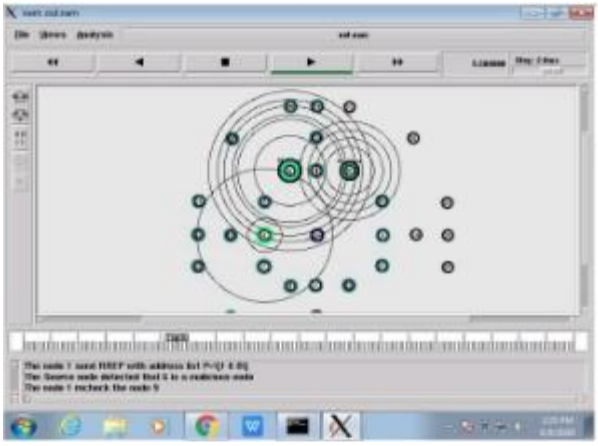
D. Packet Drop Rate for Randomly

Moved Gray Hole Nodes

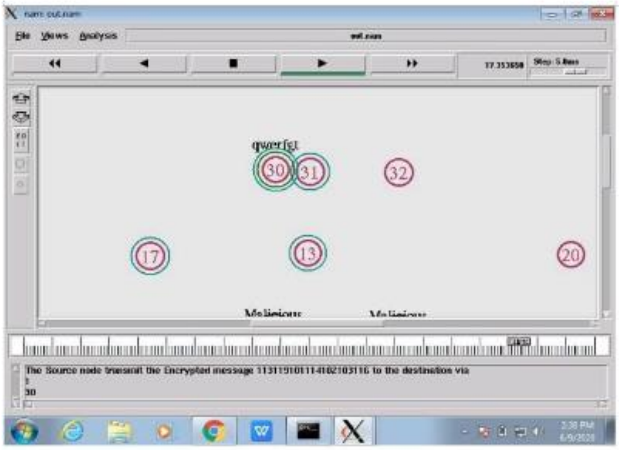
In addition to 60 normal nodes distributed, 1 or 2 gray hole nodes in network topology are considered separately. First, it was assumed that gray hole nodes are randomly moved. The total packet drop rate of one gray hole node and two gray hole nodes are as shown in figures 12 and 13 respectively and the total packet drop rate is depicted when the nodes are at different mobility speeds. Packet drop rate is also defined as the number of packets failed to reach the destination, to the number of packets transmitted from all source nodes in the network. The network might miss packets due to reasons such as congestion, mobility, traffic without gray hole nodes.







The node 1 send RREP with address list P-{1 4 8}
The Source node detected that 4 is a malicious node
The node 1 recheck the node 9



The Source node transmit the Encrypted message 113119101114102103116 to the destination via
1
30

6. CONCLUSION

In our project we've mentioned the routing security problems with MANETs and therefore the cooperative region attack in MANET. we've proposed a feasible solution for the region attacks which will be implemented on the DSR protocol. The Proposed method are often wont to find the secured routes and stop the region nodes within the MANET. As future work, we shall develop simulations to research the performance of the proposed solution supported the varied security parameters like packet delivery ratio, mean delay time, packet overhead, memory usageand scope of the region nodes.

REFERENCES

[1] -H Cho, R Chen, and K. S. Chan, "Trust threshold based public key management in mobilead hocnetworks," Ad Hoc Netw., vol. 44,pp. 58-75, Jul 2016.

[2] J. Friginal, D. de Andrés, J.-C. Ruiz, and M. Martinez, "REFRAHN:A resilience evaluation framework for ad hoc routing protocols," Comput. Netw., vol. 82, pp. 114-134, May 2015.

[3] H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hocnetworks," IEEECommun.Mag, vol.40, no. 10, pp. 70-75,Oct. 2002.

[4] L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An accurate and precise malicious node exclusion mechanism for ad hoc networks," Ad hoc Netw., vol. 19, pp. 142155, Aug. 2014.

[5] H. Xia, Z. Jia, X. Li, L. Ju, and E. H.-M. Sha, "Trust prediction and trustbased source routing inmobile ad hoc networks," Ad Hoc Netw., vol. 11, no. 7, pp. 2096-2114, 2013.

[6] Y. Yu, L. Guo, X. Wang, and C. Liu, "Routing security scheme based on reputation evaluation in hierarchical ad hoc networks," Comput Netw., vol. 54, no. 9, pp. 1460-1469, Jun.2010.

[7] N. Komninos, D. Vergados, and C. Douligeris, "Detecting unauthorized and compromised nodes in mobile ad hoc networks," Ad Hoc Netw., vol. 5, no. 3, pp. 289-298, 2007.

[8] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad hoc Netw., vol. 1, no. 2, pp. 293-315, 2003.

[9] P. Chen, S. Cheng, and K. Chen, Information fusion to defend intentional attack in InternetofThings,"IEEE Internet Things., vol. 1,no. 4, pp.337-348, Aug. 2014.

[10] X. Meng and T. Chen, "Event-driven communication for sampled-data control systems," inProc.Amer. Control Conf (ACC),vol. 1, 2013, pp.3002-3007.