IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Identification of Packet Droppers and Modifiers in Mobile Adhoc Networks for Improved Security

P. Swetha[1], Dr. P Premchand[2], Dr. P. Naveen Kumar

Associate Professor, Department of Computer Science and Engineering, JNTUH College of Engineering Jagtial, Nachupally (Kondagattu), Karimnagar, TS, India[1]

Professor, Department of Computer Science and Engineering, University College of Engineering, Osmania University, Hyderabad, TS, India[2]

Assistant Professor, Department of ECE, University College of Engineering, Osmania University, Hyderabad[3]

Abstract: The objective of this paper is to focus on security issues related to Mobile adhoc networks. Packet dropping and modifying is a common attack in wireless networks. These attacks interrupt the communication network and are difficult to identify in multi hop networks. The results present an effective scheme to identify the packet droppers and modifiers by using ranking algorithms on the DAG generated by the nodes in the network. Simulation results are presented.

Keywords: DAG, Packet Droppers, Packet Modifiers, Security, Ranking Algorithms, MANET.

I. INTRODUCTION

Security is one of the major issues in mobile networks for providing reliable communication. Packet dropping and modification are common issues that can be launched by an adversary to disrupt communication in wireless multi hop networks. Several models have been proposed to mitigate or tolerate such attacks, but very few can effectively identify the intruders to address this problem. The proposed scheme can identify misbehaving packet forwarders that drop or modify packets. The analyses have been conducted to verify the efficiency of the scheme.

To deal with packet droppers, a widely adopted method is multi path forwarding [2], [3], [4], [5] in which each packet is forwarded along multiple redundant paths, packet dropping in some paths but not all of these paths can be tolerated. To deal with packet modifiers, most of existing methods [6], [7], [8], [9] aims to filter modified messages and route within limited number of hops. These countermeasures can tolerate the packet dropping and modification attacks, but the intruders can still continue attacking the network without being caught, to locate packet droppers and modifiers in the network. It has been proposed that the nodes will continuously monitor the forwarding behaviours of their neighbours [10], [11], [12], [13], [14], [15] to determine if their neighbours are misbehaving, and the approach can be extended by using the reputation mechanisms to allow nodes to infer whether a non-neighbour node is or not [15], [16], [17], [18].

Mobile Ad Hoc Network (MANET) is a network with wireless mobile nodes. Due limitations on resources, it not only satisfies the application specific requirements such as security, reliability and timeliness, but also minimize energy consumption to increase lifetime. However, prior work exists to consider the trade-offs in the presence of malicious attackers. In a mobile network, nodes monitor the environment, detect events of interest, produce data and collaborate in forwarding data towards a sink, which could be a gateway, base station, storage node, or querying user. A network is often deployed in an unattended and unfriendly environment to perform the monitoring and data collection tasks, when it is deployed in such an environment, it does not provide physical protection and is subject to node compromise. An opponent may use various attacks to disrupt the communication. Among these attacks, two are common such as dropping packets and modifying packets, nodes drop or modify the packets that they are supposed to forward. Security is crucial for mobile networks deployed in hostile environments. The packet droppers and modifiers may be random. Detecting such attacks is very difficult and sometimes it's impossible. In this paper the monitoring and elimination of packet droppers and packet modifier nodes is done using ranking algorithms.

II. LITERATURE SURVEY

Denial-of-service (DoS) attacks on mobile networks can deplete network resources and energy without much effort on the part of an adversary. Packet dropping attacks are one category of DoS attacks. Lightweight solutions to detect such attacks on MANETs are needed. Current techniques for detecting such attacks in ad hoc networks need to monitor every node in the network. Once they detect malicious nodes that drop packets, a new path has to be found that does not include them.

This introduces Adaptive Path Selection and Loading (APSL) [2] as a multi-path data transmission scheme for mitigating the effects of misbehaving nodes in mobile ad hoc networks. In APSL, misbehavior resilience is achieved by adaptively loading Reed-Solomon (RS) coded data into

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

multiple node-disjoint paths. In order to maximize packet delivery ratio, paths are loaded according to Path State Information (PSI) which dynamically estimates the availability and stability of each path. The evaluated APSL through simulation in terms of packet delivery ratio, normalized average end-to-end delay and overhead. APSL can achieve more than 90% packet delivery ratio. Compared to adaptive single path and adaptive multi-path data forwarding with uniform loading, the packet delivery ratio is increased up to 0.9 while the end-to-end delay is reduced by a factor of 6 and the overhead is reduced by a factor of 2.

Considering a typical deployment of mobile networks, where a large number of nodes are randomly deployed in a two dimensional area. Each node generates data periodically and all these nodes collaborate to forward packets containing the data towards sink. The sink is located within the network. It is assumed that all nodes and the sink are loosely synchronized with time, which is required by many applications. Attack-resilient time synchronization schemes, which have been widely investigated in mobile networks [17], [18], can be employed. The sink is aware of the network topology, which can be achieved by requiring nodes to report their neighbouring nodes right after deployment.

III. METHODLOGY

The objective is to propose a simple yet effective scheme to catch both packet droppers and modifiers. Using node categorization algorithm it is possible to identify nodes that are droppers/ modifiers or suspicious nodes that are droppers/modifiers.

- In the initialization phase, nodes form a topology which is a Directed Acyclic Graph (DAG). A routing tree is extracted from the DAG. Data reports follow the routing tree structure.
- In each round, data are transferred through the routing tree to the sink. Each packet sender/ forwarder adds a small number of extra bits to the packet and also encrypts the packet. When one round finishes, based on the extra bits carried in the received packets, the sink runs a node categorization algorithm to identify nodes that must be bad (i.e., packet droppers or modifiers) and nodes that are suspiciously bad (i.e., suspected to be packet droppers and modifiers).
- The routing tree is reshaped at every round. As a certain number of rounds have passed, the sink will have collected information about node behaviors in different routing topologies. The information includes which nodes are bad for sure, which nodes are suspiciously bad, and the nodes' topological relationship. To further identify bad nodes from the potentially large number of suspiciously bad nodes, the sink runs heuristic ranking algorithms.

The following sections, firstly presents the algorithm for DAG establishment and packet transmission, which is followed by the proposed categorization algorithm, tree structure reshaping algorithm, and heuristic ranking algorithms. To ease the presentation, it focuses on packet droppers and assumes no node collusion. After that, it shows how to extend the presented scheme to handle node collusion and detect packet modifiers, respectively.

- Most of the bad nodes can be gradually identified with small false positive.
- Being effective in identifying both packet droppers and modifiers.

3.1 Establishment of DAG and Packet Transmission

All nodes form a DAG and extract a routing tree from the DAG. The sink knows the DAG and the routing tree, and shares a unique key with each node. When a node wants to send out a packet, it attaches to the packet a sequence number, encrypts the packet only with the key shared with the sink, and then forwards the packet to its parent on the routing tree. When an innocent intermediate node receives a packet, it attaches a few bits to the packet to mark the forwarding path of the packet, encrypts the packet, and then forwards the packet to its parent.

On the contrary, a misbehaving intermediate node may drop a packet it receives. On receiving a packet, the sink decrypts it, and thus finds out the original sender and the packet sequence number. The sink tracks the sequence numbers of received packets for every node, and for every certain time interval, which makes a single round, it calculates the packet dropping ratio for every node. Based on the dropping ratio and the knowledge of the topology, the sink identifies packet droppers based on rules derive. In detail, the scheme includes the following components.

3.2 Packet Transmission

Each node maintains a counter Cp which keeps track of the number of packets that it has sent so far. When a node u has a data item D to report, it composes and sends the following packet to its parent node Pu:< Pu ;<Ru; u; Cp MOD Ns;D; padu;0gKu; padu;1>where Cp MOD Ns is the sequence number of the packet. Ru ($0 \leq Ru \leq Np-1$) is a random number picked by node u during the system initialization phase, and Ru is attached to the packet to enable the sink to find out the path along which the packet is forwarded. (X)Y represents the result of encrypting X using key Y.

Padding's padu, 0 and padu, 1 are added to make all packets equal in length, such that forwarding nodes cannot tell packet sources based on packet length. Meanwhile, the sink can still decrypt the packet to find out the actual content. To satisfy these two objectives simultaneously, the padding's are constructed as follows:

- For a packet sent by a node which is h hops away from the sink, the length of padu,1 is log(Np)* (h-1) bits. As to be described later, when a packet is forwarded for one hop, log(Np) bits information will be added and meanwhile, log(Np) bits will be chopped off.
- Let the maximum size of a packet be Lp bits, a node ID be Lid bits and data D be LD bits. padu;0 should be Lp-Lid*2-log(Np)* h-log(Ns)-LD bits, where Lid*2 bits are for Pu and u fields in the packet, field Ru is log(Np) bits

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

long, field padu,1 is log(Np)*(h-1) bits long, and Cp MOD Ns is log(Ns) bits long. Setting padu, 0 to this value ensures that all packets in the network have the same length Lp.

3.3 Mobile Network Model Architecture

The architecture model presents the basic model of mobile network

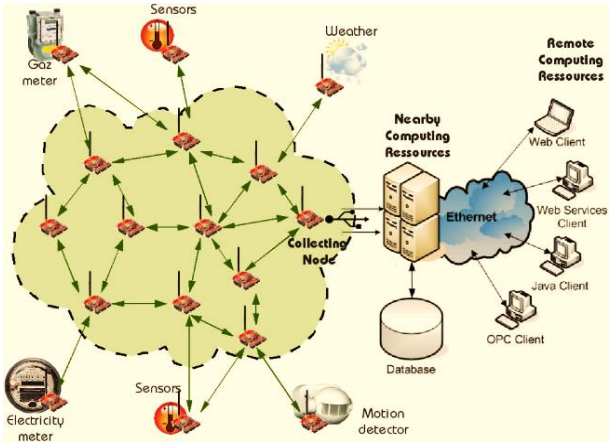

Fig.1. Mobile Network Model Architecture

Droppers: To deal with packet droppers, a widely adopted countermeasure is multi-path forwarding, in which each packet is forwarded along multiple redundant paths and hence packet dropping in some but not all of these paths can be tolerated.

Modifiers: To deal with packet modifiers, most of existing countermeasures aim to filter modified messages to route within a certain number of hops.

Sink: In each round, data are transferred through the routing tree to the sink. The sink shares a unique key with each node.

IV. SIMULATION RESULTS

This result is obtained running the in NS2 software the performance analysis is carried out

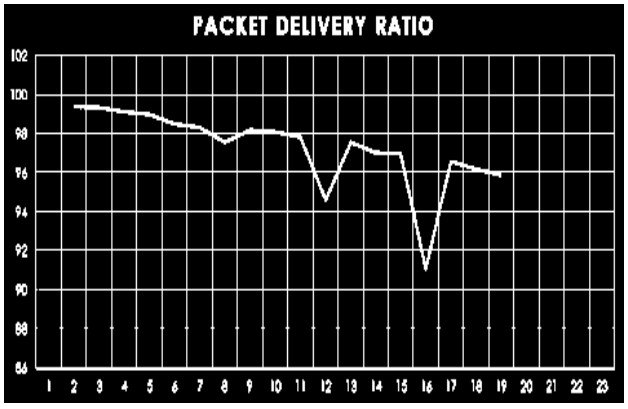

Fig2. Packet Delivery Ratio

In fig.2. Show the efficiency of the network in terms of number of packets delivered per section without data lost. The time interval to PDR is considered as 4 seconds and nodes are considered with an interval of 15. The PDR is increasing with the time interval as the bad nodes are eliminated.

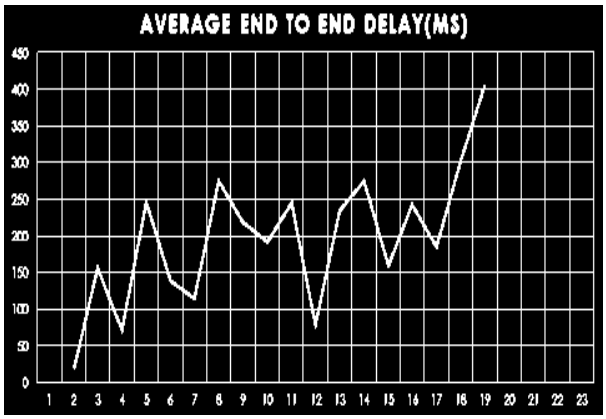

Fig3.Average End to End Delay

Fig.3. shows time interval to calculate average end to end delay which is calculated for every s 40 seconds and nodes are considered with an interval of 5.

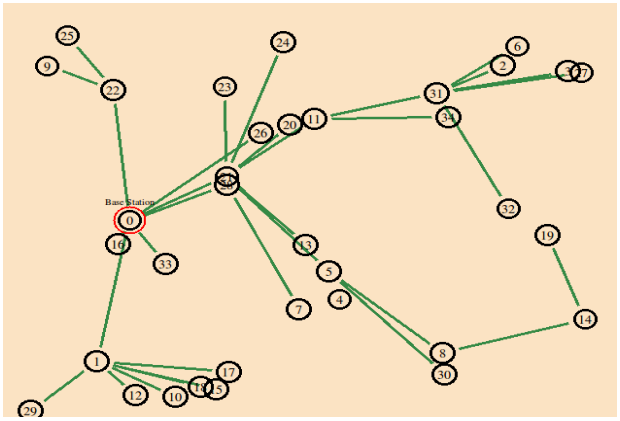

Fig. 4In the initialization phase, A routing tree is extracted from directed acyclic graph (DAG).

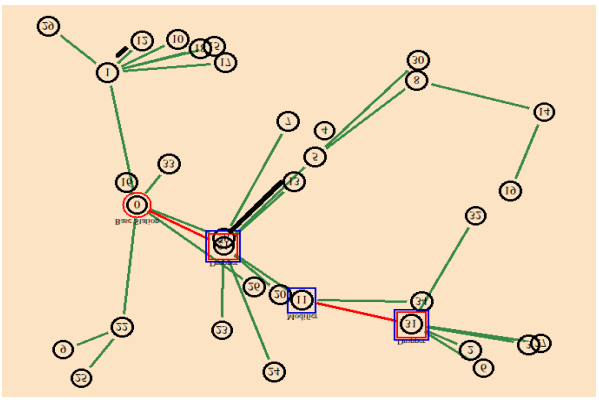

Fig. 5Identifying packet droppers and modifiersdetection in the wireless network.

V. CONCLUSION

There are several applications that provide security in mobile networks. This is one method which provides the

DOI 10.17148/IJARCCE.2016.5194

secure data transfer between the nodes. If the packet is dropped and modified that is identified in the network and is eliminated from the network. A new network model is reconstructed using DAG. With this technique there is secure transfer of data achieved and also the end to end delay is minimized and the efficiency of the system is improved as well.

REFERENCES

[1]. Catching Packet Droppers and Modifiers in Wireless Sensor Networks by Chuang Wang, Taiming Feng, Jinsook Kim, Guiling Wang, Member, IEEE, and Wensheng Zhang,

[2] A.Gantes and j. stucky, "A platform on a Mobile Ad hoc Network challenging collaborative gaming," international symposium on collaborative technologies and systems, 2008.

[3] K.U. R. Khan, R. U. Zaman, and A. V. G. Reddy, "Integrating Mobile Ad Hoc Networks and the Internet challenges and a review of strategies," presented at the 3rd International Conference on Communication Systems Software and Middleware and Workshops, COMSWARE, 2008.

[4] M.Suguna and P. Subathra, "Establishment of stable certificate chains for authentication in mobile ad hoc networks," presented at the International Conference on Recent Trends in Information Technology (ICRTIT), 2011.

[5] H.Nishiyama, T. Ngo, N. Ansari, and N. Kato, "On Minimizing the Impact of Mobility on Topology Control in Mobile Ad Hoc Networks," Wireless Communications, IEEE Transactions, 2012.

[6] F.D. Rango, M. Fotino, and S. Marano, "EE-OLSR: Energy Efficient OLSR routing protocol for Mobile ad-hoc Networks," presented at the Military Communications Conference, MILCOM, 2008.

[7] H.Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks,," Communications Magazine,IEEE, 2002.

[8] Y.Z.a and W. Lee, "Intrusion Detection in Wireless Ad-Hoc networks," presented at the 6th Int'l. Conf. Mobile Comp. Net., MobiCom, 2000.

[9] F.S.a and R. Anderson, "The Resurrecting Ducking: Security Issues for Ad-Hoc Wireless Networks," 7th Int'l. Wksp on Security Protocols. Proc., LNC, 1999.

[10] X.Zhao, Z. You, Z. Zhao, D. Chen, and F. Peng, "Availability Based Trust Model of Clusters for MANET," presented at the 7th International Conference on Service Systems and Service Management (ICSSSM), 2011.

[11] E.C.H.Ngai and L. M. R, "Trust and clustering-based Authentication Services in Mobile ad hoc networks," presented at the proceeding of the 24th international conference on Distributed Computing systems Workshops 2004.

[12] W.Lou, W. Liu, and Y. Fang, "SPREAD: enhancing data confidentiality in mobile ad hoc networks," presented at the Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, 2004.

[13]S.Rana and A. Kapil, "Security-Aware Efficient Route Discovery for DSR in MANET," Information and Communication Technologies, Communications in Computer and Information Science, vol. 101, pp. 186-194, 2010.

[14] X.Lv and H. Li, "Secure group communication with both confidentiality and non-repudiation for mobile ad-hoc networks," Information Security, IET, vol. 7, 2013.

[15] S.a.A.k.G, H.o.d.R.m, and S. sharma, "A Comprehensive Review of Security Issues in Manets," International Journal of Computer Applications vol. 69 2013.

[16] V.P.and R. P. Goyal, "MANET: Vulnerabilities, Challenges, Attacks, Application," IJCEM International journal of Computational Engineering & management, vol. 11, 2011.

[17] A.MISHRA, R. Jaiswal, and S. Sharma, " A novel approach for detecting and eliminating cooperative black hole attack using advanced DRI table in Ad hoc Network," presented at the 3rd International Conference on Advance Computing Conference (IACC), 2013

[18] N.-W. Lo and F.-L. Liu, "A Secure Routing Protocol to Prevent Cooperative Black Hole Attack in MANET," in Intelligent Technologies and Engineering Systems. vol. 234, J. Juang and Y.-C. Huang, Eds., ed: Springer New York, 2013, pp. 59-65.