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. 10, October 2014, pg.114 – 120

RESEARCH ARTICLE

Colluding Detection of Misbehaving Nodes in MANET

[1]Vasantha Laxmi.CH
PG Scholar, Dept. of IT, SNIST, Hyderabad, Telangana, INDIA
vasantha0409@gmail.com

[2]Kranthi Kumar.K
Assistant Professor, Dept. of IT, SNIST, Hyderabad, Telangana, INDIA
kranthikathula@gmail.com

Abstract— with the increasing popularity of portable devices, wireless ad-hoc networks have been widely used to achieve better connectivity at places where an infrastructure is not immediately available or cannot be directly used. Its infrastructure less property and the easy deployment along with the self-organizing nature makes them useful for many applications. Nodes in MANET are with limited battery power and resources. Where few nodes behaves selfish to save their resources by expecting services from other neighboring nodes but refusing to provide any service to its neighbors or misbehaves by colluding, since routing requires cooperation of nodes it is highly important to provide incentives for them to cooperate. There exists extensive work in Mobile Ad hoc Networks (MANETs) on security measures as well as correctness of the estimation of the position of a node despite attacks from adversaries.

Keywords— Mobile Ad hoc Networks (MANETs), Colluding adversaries, Collusion, Attacker Detection

I. INTRODUCTION

The recent few years have witnessed a growing interest in mobile ad hoc network (MANET) which is a spontaneous self-organized infrastructure-less network or decentralized administrated network, wherein the networking activities like routing and data transmission are carried on by the nodes themselves in a collaborative manner. Evolution of wireless networking and mobile computing hardware have resulted in wide spread usage of MANETs in many distributed applications Digital battlefield, fast response to disasters, context aware computing, Soldiers relaying information for situational awareness on the battlefield, business associates sharing information during a meeting; attendees using laptop computers to participate in an interactive conference; and emergency disaster relief personnel coordinating efforts after a fire, hurricane, or earthquake and mobile commerce are examples of a growing list of potential applications MANETs. The other possible applications [1] include personal area and home networking, location-based services, and sensor networks.

Its nodes are equipped with wireless transmitters/receivers using antennas which may be unidirectional (broadcast), highly-directional (point-to-point), or some combination without the usage of any routers. In other words, nodes themselves act as routers as well as

source and they depend on each other for forwarding packets from a source to a destination. At a given time, the system can be viewed as a random graph due to the movement of the nodes; MANETs may operate separately or can be interfaced with fixed network through gateways.

These characteristics have made the design and management of MANETs significantly challenging in comparison to contemporary networks. Confidentiality, authenticity, availability and integrity are typical security goals of MANETs. There are varieties of attacks that target the loopholes of MANETs, or one/more of these security goals. Attacks may be external such as traffic jamming to node damaging, or internal such as collusion among some nodes to reveal the fundamentals of the employed security scheme. The main problem of communication in a MANET results from the inconsistency of the nodes to transmit the packet to some destination. This inconsistency results from a number of factors: Firstly, each node's transmission range is limited and nodes are mobile. Hence the dynamic nature of the network may cause a node which forwarded the data packets for some source/destination pair at some point of time, not being able to do so at a later point of time due to mobility which may effect its transmission range. Secondly, the limited battery power of the nodes may effect its packet forwarding behavior.

Secure localization scheme, that is, one that guarantees the accuracy of computed locations, is absolutely required. But, in civilian ad hoc networks, nodes often belong to different nodes and have their own interests; they may not want to behave cooperatively. Consequently, it is highly important to provide incentives for nodes to cooperate.

Usually, there are two steps in a localization process: information acquisition and position calculation. Most adversaries attack the step of a localization process where in an attacker can either corrupt normal nodes in network by sending false localization information, or pretend to be a legitimate node in order to falsify its identity, so that it replay communication data to create collusion. Such attacks will lead to inaccurate localization calculations (regardless of whether it is a centralized authority node that calculates the location of a location-unknown node, or such a node calculates its own location locally). Consequently, security measures have been extensively studied in order to make estimated positions correct despite attacks from an adversary. But several questions remain, in particular: a) what happens when several adversaries collude?

II. RELATED WORK

In MANET, cooperation is very important to support the basic functions of the network. Location disclosure attack where in an attacker gives location details of nodes in network or the structure of the network itself. Misbehaving node gathers the node location information, route map, and then plans further attack scenarios. Traffic analysis, is one of the security attack against MANET where in adversary nodes try to find identities of communication parties and analyze traffic with in network to learn traffic pattern and track changes in it by continuous observation. Revealing such information by Misbehaving node in network is devastating in security sensitive scenarios. Zhang [2] proposed a design for IDS and response mechanisms for MANET. Marti [3] proposes two mechanisms to improve throughput in the presence of nodes in network but remained unsolved. These methods are watchdog and path rater, Similarly, Buchegger and Le Boudec's solutions [4, 5] also use an approach based on reputation. In their solutions, each node has a state machine for the reputation of other nodes; the nodes update their states according to their observations and received reports of other nodes' behavior.

Routing messages plays vital role in mobile network communications, as each message exchanged between nodes known as packets need to be exchanged quickly via all participating nodes, traversing from source to the destination. In the routing problem, we need a routing scheme that computes the lowest cost path despite of the fact that selfish nodes can make false claims about their costs. In the packet forwarding problem, we need a protocol that stimulates selfish nodes to forward packets. Ben Salem et al. [6] addresses the packet forwarding problem in multi-hop cellular networks, using a protocol based on symmetric key cryptography. Routing attacks can target the phase of path identification or maintenance of that route by not following the specifications of the routing protocols. An attacker may modify packets exchanged among some nodes, while leaving the packets from the other nodes unaffected, which limits the suspicion of its identity. A compromised intermediate node may work all alone, or a set of compromised nodes work in collusion and carry out attacks such as generating bogus location information which results in disruption or degradation services

In Collaborative Collusion [7], the CCAM model is proposed. In that model all malicious nodes can collaborate with each other to alter the location information they receive and/or jointly forward it. The authors present a solution to detect such malicious nodes. In fact, attacker detection is performed only by this base station. Such calculation at a central node has several drawbacks. Furthermore, beyond location information, threat of collaborative attacks on MANETs by colluding adversaries continuously and a number of mechanisms have been designed for the defense against these attacks. Collaborative intrusion detection systems have been designed in [8] which assume a clique or a cluster network structure. Another approach involves certain ideas borrowed from immune systems for the collaborative detection of adversaries [9]. Intrusion detection system called as honesty based IDS which makes collaborative decisions based upon multiple threshold values including rewards and penalties for packet forwarding has been proposed in [10].

This paper is structured as follows. In Section 3 we describe our proposed approach followed by Evaluation of proposed system in section 4 and in section 5 conclusions are given.

III. PROPOSED APPROACH

The wireless nature of MANETs renders them susceptible to various attacks, especially when deployed in hostile and unattended environments. A misbehaving adversary may try to gain access to those messages that are exchanged in the system, intercept these messages as well as inject false messages. In this paper we mainly consider an adversary that tries to manipulate the system through compromising some network nodes.

Threat Model

In our system, threat occurs only when two or more nodes trying to collude with each other so as to generate bogus location proofs. For example, when a misbehaving node M1 from San Francisco needs to prove herself in New York City (NYC), she can have another colluding node M2 to generate bogus locations behalf of it, with location tag of New York City. Whereas, such attacks can be easily identified by observing the location traces and by examining the messages exchanged between colluders as well as the time and location consistency along the moving trajectory.

In this section, we describe the working of our approach. Our approach makes the following assumptions, multiple malicious nodes exist in our adversarial models and these nodes can communicate through a side channel. They synchronize and act as colluding adversaries to hide location, or generate bogus location information. The nodes can impersonate each other and collaborate such that one of them misbehaves and the remaining nodes help it to avoid detection.

We define a neighborhood of a network, which are in the transmission range. In order to collude, two nodes must be in the transmission range of one another, otherwise they have to collude through a third party. Collusion is most likely to occur when two neighboring nodes are compromised. The compromise of a node implies that the node has been captured by an adversary and can be manipulated. Thus, when two nodes in the same neighborhood are compromised, they may be manipulated to collude. As a result of collusion, the two colluding nodes hide location of legitimate node.

In Figure1 (a), a sample network is considered where S is source node and D is Destination node, remaining are intermediate nodes in given network. And the communication path is as shown, $S \rightarrow A \rightarrow B \rightarrow C \rightarrow D$. To implement our idea, we need to consider how a node can convince other nodes about its own action. There are two basic approaches: Either the node convinces other nodes by showing messages it has sent, or the node does so by showing messages it has received. (Of course, it can also use a combination of the two basic approaches.) Among the sent messages, the only one related to its own action is its message to the source node S, which contains its claimed cost. In particular, there is a message received by the node which contains information about its own action.

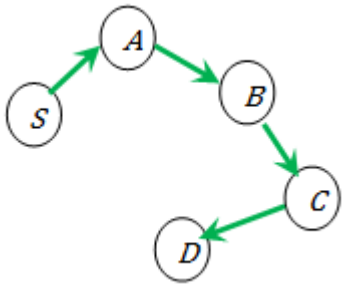
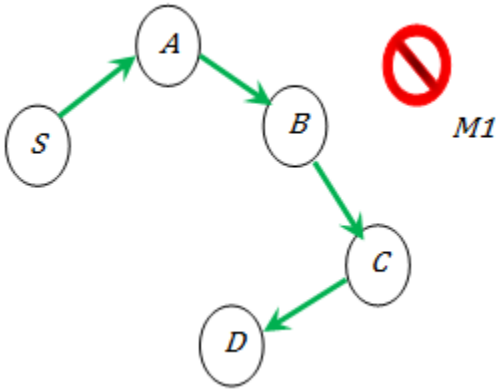


Fig 1: (a) Sample Network



(b) Malicious node $M1$ entered transmission range

In Figure1 (b), a Malicious node *M1* entered in Transmission range of network. Now *M1* compromises node *B* and take the position of node *B* in network i.e, *B* is under control of *M1* which is shown in figure 2. Having this common behavior, further categorization depends on how an attacker lies about its location during the localization process:

1. A liar lies about its location by using a randomly generated fake location;
2. A liar lies about its location by giving out a fake location: in cooperation with two other attackers.

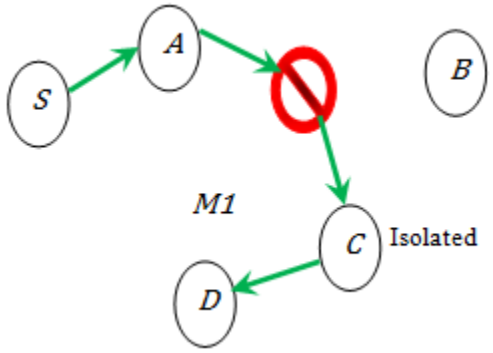


Fig 2: Malicious node *M1* in path between *S* and D.

The following scenarios can be identified for the compromised nodes to collude:

a) The compromised nodes have direct communication links: In such a case, collusion can be very subtle and hard to prevent.

b) The compromised nodes can only communicate through multi-hops: This would require the compromised nodes to be aware of the location/ID of other compromised nodes.

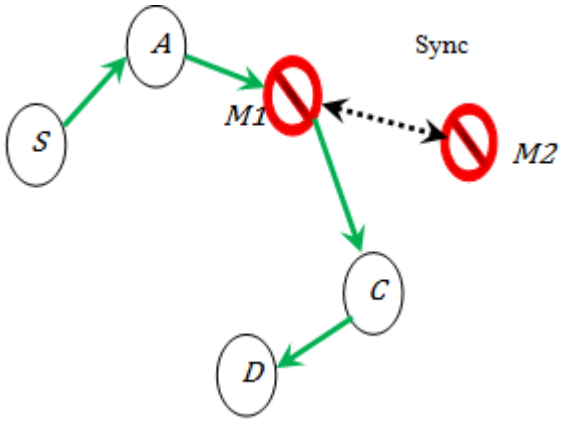


Fig 3: Malicious node *M2* in synchronous with *M1*.

Collusion implies that two or more parties collaborate by secretly sharing their knowledge in order to gain access to certain information that they are not authorized to have. In our system a collusion attack can be possible when compromised nodes are in the transmission range of one another. For example, imagine that malicious nodes *M1* and *M2* are trying to collude .They are in synchronous with each other and trying to make node *C* to misbehave.

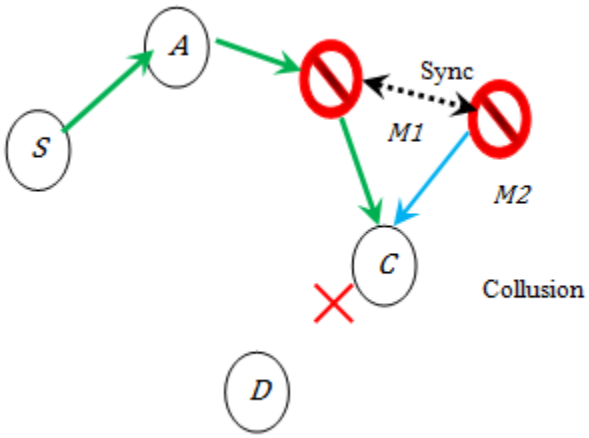


Fig 4: Collusion in path between *S* and *D.*

A. Detection of Colluding node

In order to find Colluding node we calculate the *Trust Level (TL)* of every node in network. Calculating the trust level of a location proof involves the examination of its surrounding location, as well as large amount of redundant calculations between individual location proofs. Let us consider preselected threshold value as 0.5(50%), meaning if trust value is at least 50% then node is considered as good node, else compromised node.

$$TL=\frac{N_{proof}}{N_{neighbor}}$$

Where N_{proof} is number of location proofs with node currently

And $N_{neighbor}$ is number of surrounding nodes

By using TL we find misbehaving node in figure 4,checking TL for node C as N_{proof} =1, which is given by $M1$ and $N_{neighbor}$ =4,as it is surrounded by 4 nodes S,A,B,D.

$TL=\frac{N_{proof}}{N_{neighbor}}=\frac{1}{4}$ =0.25

Since the trust level TL is lesser than preselected threshold, C is considered as a colluding node.

Step 1: S maintains TL of each node per route and send to D
Periodic proactive routing messages provide this detail of node.

Step 2: intermediate nodes per route append their own information

Step 3: D collects the traffic information from incoming routing messages .

Step 4: D detects misbehaving nodes by recognizing the number of bytes received differs significantly from the number of bytes originated by the S.

Step 5: Maintaining graph and counter by D,S respectively.

IV. EVALUATIONS

Consider a random wireless network with 100 nodes distributed in a terrain area of 3000 by 3000 meters. Nodes use IEEE 802.11 as the MAC layer protocol. In a randomly generated network topology we only include the labels of a few nodes. A line between two nodes means that the two nodes are in the communication range of each other. We have an evaluation done on the random wireless network to illustrate the effect of collusion and show that this proposed attack cannot be detected by previous proposed malicious detection schemes [11] [12].

In this work, we defined the *Trust Level* as the detection of a legitimate node as being malicious. To show how previously proposed detection scheme will perform against our proposed model, we used the TL as a performance metric, which is defined as, the ratio of the number of location proofs of a scheme in the existence of an attack to the total number of surrounding nodes in the network.

In our simulation, we allow attacker node to have the ability to attack our proposed network many times but with in different time slots through the simulation time carried out, in other words, in one time the malicious nodes will work as legitimate nodes, and other time they will launch the attack.

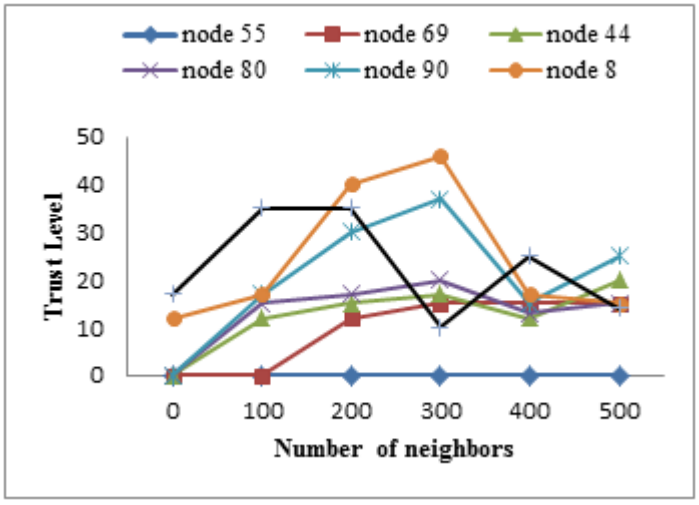


Fig 5: Trust Level of Nodes as a Function of total nodes.

Figure 5 and Figure 6 show Trust Level and Collusions of seven typical nodes during the evaluation, respectively. Generally, nodes locating in the central part of the network or at a position connecting two node-dense areas (like node 69 and node 80) get higher collusion.

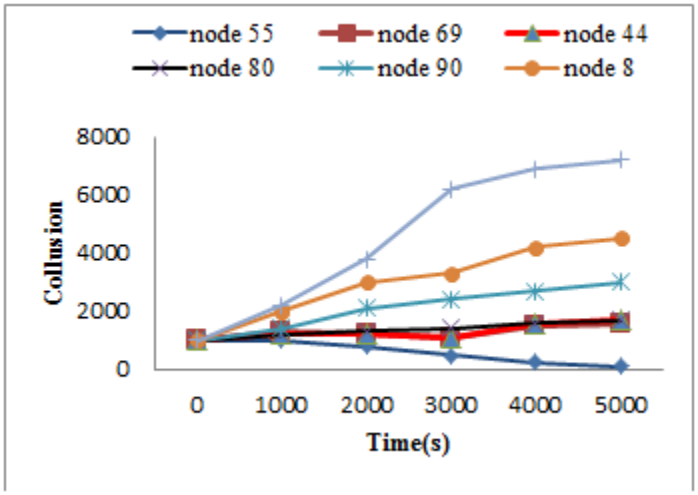


Fig 6: Collusion as a Function of Simulation Time.

In contrast, nodes like 55 have much lower collusion, because they have less chance to be compromised in network as they are most influential nodes in the network (i.e., who inter connects with most others)[13].For each number of colluding nodes, we have 20 runs of the experiment. In each run, the source node, the destination node, and the set of colluding nodes are randomly selected.

V. CONCLUSION

Despite its applicability to multiple applications, it cannot be considered as an alternative to a wired network and it demands a lot of research on collusion issues .Our proposed mechanism efficiently detects the colluding adversaries without the need of having the source node share a secret with every intermediate node unlike the approach proposed in [14]. Many attacks make the estimated positions incorrect. Such incorrect positions may lead to severe consequences in many applications. Thus, security measures have been studied extensively in order to make the estimated positions correct despite the attacks from an adversary. But very little work has been done on investigating how colluding attackers can change the behavior of known attacks or even create new attacks. In this paper, we present an attack model that allows three types of colluding attackers to attack the secure localization process and/or the attacker detection process.

REFERENCES

[1] C. Papadimitriou. Algorithms, games, and the Internet. In Proceedings of the 33rd Annual
Symposium on Theory of Computing, pages 749-753, Heraklion, Crete, Greece, Jul. 2001.6.

[2] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-hoc Networks, *Proc. of the Sixth Annual International Conference on Mobile Computing and Networking* (MOBICOM), Boston, 2000.

[3] S. Marti, T. Giuli, K. Lai, and M. Baker, Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, *Proc. of the Sixth Annual International Conference on Mobile Computing and Networking* (MOBICOM), Boston, 2000.

[4] S. Buchegger and J.-Y. Le Boudec. Nodes bearing grudges: Towards routing security, fairness, androbustness in mobile ad hoc networks. In Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing (EUROMICRO-PDP), Canary Islands, Spain, Jan.2002.

[5] S. Buchegger and J.-Y. Le Boudec. Performance analysis of the CONFIDANT protocol (Cooperation of nodes: fairness in dynamic ad-hoc networks). In Proceedings of the Third ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Lausanne, Switzerland, Jun. 2002.

[6] N. Ben Salem, L. Buttyan, J. P. Hubaux, and M. Jakobsson. A charging and rewarding scheme for packet forwarding in multi-hop cellular networks. In 288 Proceedings of the Fourth ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc), Annapolis, MD, Jun. 2003.

[7] Jiang, J., Han, G., Shu, L., Chao, H., and S. Nishio.: A novel secure localization scheme against collaborative collusion in wireless sensor networks. In: 7th International Wireless Communications & Mobile Computing Conference, pp. 308-313. July 2011.

[8] N. Marchang, and R. Datta, "Collaborative techniques for intrusion detection in mobile ad-hoc networks," Ad Hoc Netw. 6(4), pp. 508-523, 2008.

[9] K. Yeom and J. Park, "An immune system inspired approach of collaborative intrusion detection system using mobile agents in wireless ad hoc networks", in International conference of Computational intelligence and security, 2005.

[10] P. Sen, N. Chaki, R. Chaki, "HIDS: Honesty-Rate Based Collaborative Intrusion Detection System for Mobile Ad-Hoc Networks," Computer Information Systems and Industrial Management Applications (CISIM), pp.121-126, 2008.

[11] I. Khalil, S. Bagchi, C. Nina-Rotaru, "DICAS: Detection, Diagnosis and Isolation of Control Attacks in Sensor Networks," SecureComm 2005, pp.89-100.
[12] S. Marti, T.J. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," MobiCom 2000, New York, NY, USA, pp.255-265.
[13] Z. Zhu and G. Cao, "APPLAUS: A Privacy-Preserving Location Proof Updating System for Location-Based Services," Proc. IEEE INFOCOM, 2011.
[14] Weichao Wang Bharat Bhargava Mark Linderman "Defending against collaborative packet drop attack.
[15] H. Yang, et al., "Security in Mobile Ad-Hoc Wireless Networks: Challenges and Solutions," IEEE Wireless Communications Magazine, February 2004.

