

An Enhanced Adaptive Security Protocol For Replica Attacks In Mobile Adhoc Networks

*M.Praveena¹, R.M.Thiriburabhavan², R.M.Bhavadharini³
, Dr.S.Karthik⁴*

¹PG Scholar, Dept of CSE, SNS College of Technology, Coimbatore.

²PG Scholar, Dept of CSE, SNS College of Technology, Coimbatore.

³Prof, Dept of CSE, SNS College of Technology, Coimbatore,

⁴Prof & Dean, Dept of CSE, SNS College of Technology, Coimbatore.

Abstract:

Mobile Adhoc Network represents the complex distributed systems for data transmission. Mobile node requires a unique, distinct, and persistent identity. Since, MANET is a wireless medium it can expect more security and vulnerability problems. One of the major security problems is attacks. There are many attacks in MANET one of the attack is node replica. A node replica attack can create more than one identity on a single node in order to deploy an attack on the network to impose adverse effect by switching identities. This attack pose a serious threat such as traffic disturbance and packet delay .In this proposed system, it propose a Novel adaptive routing security mechanism using Clustering and Classification techniques to detect the new identities of replica attacks without using centralized mobile sinks such as geographical positioning system. Through the help of extensive simulations and experiments, they are able to demonstrate that the proposed mechanism estimates the attack identities with good accuracy even in the presence of mobility.

KEY WORDS: MANET, Sybil attack, node replica, GPS.

I.Introduction:

Mobile Ad Hoc Network (MANET) is a self-creating, self-organizing and self-administering wireless network. MANET is a collection of

communication devices or nodes that wish to communicate without any fixed infrastructure and pre-determined organization of available links. [3]The nodes in MANET themselves are responsible for dynamically discovering other nodes to communicate. It is a self-configuring network of mobile nodes connected by wire-less links the union of which forms an arbitrary topology. The nodes are free to move randomly and organize them-selves arbitrarily thus, the network's wireless topology may change rapidly and unpredictably.[5]

Based on the security informaion, Ad hoc wireless network attacks are basically divided into active attack and passive attack.[7] Active attacks which are really difficult to locate or identify because these attacks are more sophisticated. Passive attacks use eavesdropping or monitoring attacks use eavesdropping or monitoring transmissions to obtain information.Network layer is responsible for routing packet through a network or establishing a connection between two entities over many other intermediate systems.[10] It is used for addressing, routing, device location and handover between different networks. Transport layer is used in the reference model to establish an end to end connection.the attacks in network layer are Sybil,

Flooding, Black Hole, Grey Hole, Worm Hole, Link Spoofing, Link Withholding, Location disclosure.[12] The Sybil attack in computer security is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks. A reputation system's vulnerability to a Sybil attack depends on how cheaply identities can be generated, the degree to which the reputation system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the reputation system treats all entities identically. Evidence shows large-scale Sybil attack can be carried out in a very cheap and efficient way in the realistic system like BitTorrent Mainline DHT.[9]

The characteristics of selfish nodes as follows:

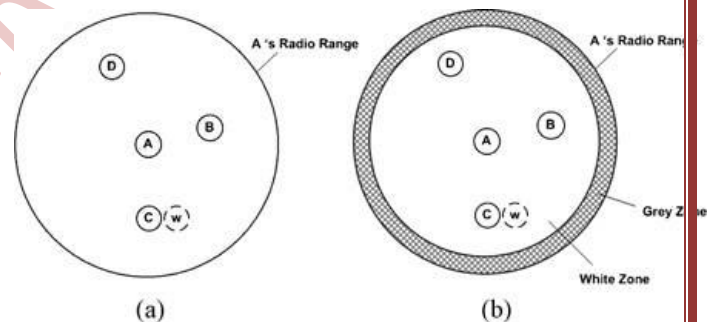
- Do not participate in routing process: A selfish node drops routing messages or it may modify the Route Request and Reply packets by changing TTL value to smallest possible value.
- Do not reply or send hello messages: A selfish node may not respond to hello messages, hence other nodes may not be able to detect its presence when they need it.
- Intentionally delay the RREQ packet: A selfish node may delay the RREQ packet up to the maximum upper limit time. It will certainly avoid itself from routing paths.
- Dropping of data packet: A selfish nodes may participate in routing messages but may not relay data packets.

ii. Related Work

The scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities.[13] First, it demonstrate the entry and exit behavior of legitimate nodes and Sybil nodes using simulation and testbed experimentation. Second, it define a threshold that distinguish between the legitimate and Sybil identities based on nodes' entry and exit behavior.

Third, it tune the detection threshold by incorporating the RSS data fluctuation taken from our testbed experimentation. Fourth, it evaluate our scheme using extensive simulations, and the results

show that it produces about 90% true positives (detecting a Sybil node as Sybil) and about 10% false positives (detecting a normal node as a Sybil node) in mobile environments.[14] The scheme can be applied to both scenarios of Sybil attacks, i.e., whether the new identities are created one after the other or simultaneously make no difference to the detection process. The detection scheme can work as a standalone scheme, but could equally be deployed as an add-on to existing schemes, for example it could be incorporated into a reputation-based system, i.e., the detected Sybil identities from the MAC layer will be plugged into the reputation-based system on network layer.[3] The proposed scheme does not use localization technique for Sybil attack detection and hence does not need any directional antennae or any GPS equipment, as used in [8] and [9]. Unlike [10] and [11], the proposed scheme does not use centralized trusted third party. In our scheme, nodes share and manage identities of Sybil and non-Sybil nodes in distributed manner.



Each node maintains a list of neighbors in the form <Address, Rss-List <time, rss>> and records the RSS values of any directly received or overheard frames of 802.11 protocol, i.e., RTS, CTS, DATA, and ACK messages. In other words, each node will capture and store the signal strength of the transmissions received from its neighboring nodes. This can be performed when a node either takes part in the communication directly with other nodes acting as a source or a destination or when a node does not take part in the direct communication.

ii.Proposed Approach

The main characteristic of MANET is the dynamic changing topology, here in the network

some nodes reserve their own energy without forwarding packets to the neighbour nodes and such nodes are called as selfish nodes. These selfish nodes are detected and isolated from the network by calculating the credit risk value for each node. Then SCF Tree is constructed for the nodes that are non-selfish and then nodes with higher priority is allocated replica for forwarding packets to the destination. A periodic update is performed for every certain threshold value which keeps the network free from selfish nodes.

i) Establishing Mobile Ad hoc Networks:

First, construct and Mobile Ad hoc Networks with several nodes which is self organizing type. Each node in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic with various entity like identity. Such networks may operate by themselves or may be connected to the larger Internet. Because of the infrastructure-less architecture of MANET, our risk-aware response system is distributed, which means each node in this system makes its own response decisions based on the evidences and its own individual benefits. Therefore, some nodes in MANET may isolate the malicious node, but others may still keep in cooperation with due to high dependency relationships

ii) Modelling the Attack types:

In terms of attack vectors, a malicious node can disrupt the routing mechanism in the following simple ways: It changes the contents of a discovered route, modifies a route reply message, and causes the packet to be dropped as an invalid packet. It validates the route cache in other nodes by advertising incorrect paths, and refuses to participate in the route discovery process. finally, it modifies the contents of a

data packet or the route via which the data packet is supposed to travel or behave normally during the route discovery process but is dropped. Any node can either modify the protocol messages before forwarding them, or create false messages or spoof an identity.

Therefore, the attacker can abuse the properties of the selection algorithm to be selected as MPR. The worst case is the possible selection of the attacker as the only MPR of a node. Or, the attackers can give wrong information about the topology of a network (TC message) in order to disturb the routing operation.

iii) Exploring the node replicas in the dynamic Environment

The low-cost, off-the-shelf hardware components in unshielded sensor-network nodes leave them vulnerable to compromise. With little effort, an adversary may capture nodes, analyze and replicate them, and surreptitiously insert these replicas at strategic locations within the network. Such attacks may have severe consequences; they may allow the adversary to corrupt network data or even disconnect significant parts of the network. Previous node replication detection schemes depend primarily on centralized mechanisms with single points of failure, or on neighborhood voting protocols that fail to detect distributed replications. To address these fundamental limitations, we propose two new algorithms based on emergent properties, i.e., properties that arise only through the collective action of multiple nodes. Randomized Multicast distributes node location information to randomly-selected witnesses, exploiting the birthday paradox to detect replicated nodes, while Line-Selected Multicast uses the topology of the network to detect replication. Both algorithms provide globally-aware, distributed node-replica detection, and Line-Selected Multicast displays particularly strong performance characteristics. This show that emergent algorithms represent a promising new approach to sensor

network security; moreover, our results naturally extend to other classes of networks in which nodes can be captured, replicated and re-inserted by an adversary.

iv) Collaborative Clustering mechanism

The most straightforward detection scheme requires each node to send a list of its neighbors and their claimed locations to the base station. The base station can then examine every neighbor list to look for replicated nodes as follows

Node replication Clustering algorithms may be classified as listed below:

- Hierarchical Clustering
- Probabilistic Clustering.

By introducing the model of the proposed cluster-based revocation scheme, which can quickly revoke attacker nodes upon receiving only one accusation from a neighboring node. The scheme maintains two different lists, warning list and blacklist, in order to guard against malicious nodes from further framing other legitimate nodes. Moreover, by adopting the clustering architecture, the cluster head can address false accusation to revive the falsely revoked nodes. Owing to addressing only the issue of node revocation, not node distribution, the scheme assumes that all nodes have already received certificates before joining the network. On the other hand, we focus on the procedure of node revocation once a malicious attacker has been identified, rather than the attack detection mechanism itself.

v) Reliability-Based Node Classification:

According to the behavior of nodes in the network, three types of nodes are classified according to their behaviors: legitimate, malicious, and attacker nodes. A legitimate node is deemed to secure communications with other nodes. It is able to correctly detect attacks from malicious attacker nodes and accuse them positively, and to revoke their node structure in order to guarantee network security. A malicious node does not execute protocols to identify misbehavior, vote honestly, and revoke malicious attackers.

In particular, it is able to falsely accuse a legitimate node to revoke its permission successfully. The so-called attacker node is defined as a special malicious node which can launch attacks on its neighbors to disrupt secure communications in the network. In this scheme, these nodes can be further classified into three categories based on their reliability: normal node, warned node, and revoked node. When a node joins the network and does not launch attacks, it is regarded as a normal node with high reliability that has the ability to accuse other nodes. Moreover, we should note that normal nodes consist of legitimate nodes and potential malicious nodes. Nodes that are listed in the warning list are deemed as warned nodes with low reliability. Warned nodes are considered suspicious because the warning list contains a mixture of legitimate nodes and a few malicious nodes. Warned nodes are permitted to communicate with their neighbors with some restrictions, e.g., they are unable to accuse neighbors any more, in order to avoid further abuse of accusation by malicious nodes.

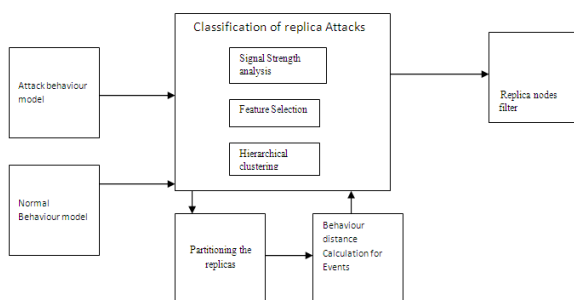


Fig 1. Diagram of Clustering

IV. Conclusion

In contrast to the network viewpoint, we have addressed the problem of selfish nodes from the replica allocation perspective. This problem is known as selfish replica allocation. This work was motivated by the fact that a selfish replica allocation could lead to overall poor data accessibility in a MANET. We

have proposed a selfish node detection method with novel replica allocation to handle the selfish replica allocation appropriately techniques and a timer based acknowledgement technique in eliminating misbehaving nodes. The proposed strategies are inspired by the real-world observations in economics in terms of credit risk and in human friendship management in terms of choosing one's friends completely at one's own discretion. The notion of credit risk is applied from economics to detect selfish nodes. Every node in a MANET calculates credit risk information on other connected nodes individually to measure the degree of selfishness. Since traditional replica allocation techniques failed to consider selfish nodes, novel replica allocation technique is also proposed with timer based acknowledgement scheme. When the number of misbehaving nodes exceeds the minimum count, then this scheme would be a better one to detect the misbehaviors at the source. Extensive simulation shows that the proposed strategies outperform existing representative cooperative replica allocation techniques in terms of data throughput, communication overhead, and end to end delay.

References

1. Dipali Koshti and Supriya Kamoji, "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks", IJSCE, vol. 1, issue - 4, September 2011.
2. Jae-Ho Choi et al., "Handling Selfishness in Replica Allocation over a Mobile Ad Hoc Network", IEEE Transactions On Mobile Computing, Vol. 11, No. 2, February 2012.
3. Jerzy Konorski and Rafał Orlikowski, "A Framework for Detection of Selfishness in Multihop Mobile Ad Hoc Networks", Journal of Telecommunication and Information Technology, February 2009.
4. Kejun Liu, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, "An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", September 2006.
5. Khairul Azmi Abu Bakar, "Contribution Time-Based Selfish Node Detection Scheme, 2001.
6. Mehdi Kargar and Mohammad Ghodsi, "Truthful and Secure Routing in AdHoc Networks with Malicious and Selfish Nodes", International Journal of Security and its Applications Vol. 3, No. 1, January, 2009.
7. Mohammad Wazid, Rajesh Kumar Singh and R. H. Goudar, "A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques", International Journal of Computer Applications® (IJCA), International Conference on Computer Communication and Networks CSI-COMNET-2011.
8. Prasanna Padmanabhan, Le Gruenwald, Anita Vallur and Mohammed Atiquzzaman, "A survey of data replication techniques for mobile ad hoc network databases", the VLDB Journal, 2008.
9. Rajeev Kumar, and Prashant Kumar, "Replica Allocation Technique Based on Clusters for MANETs", International Conference on Emerging Trends in Computer and Electronics Engineering (ICETCEE'2012) March 24-25, 2012.
10. Ramasamy Murugan and Arumugam Shanmugam, "A Timer Based Acknowledgement scheme for Node Misbehavior Detection and Isolation in MANET", International Journal of Network Security, Vol.15, No.1, PP.182-188, January 2013.
11. Sangheetha Sukumaran, Venkatesh.J and Arunkorah, "A Survey of Methods to mitigate Selfishness in Mobile Ad hoc Networks", International JICT, vol. 1, no. 2, June 2011.
12. Shailender Gupta, Nagpal.C.K. and Charu Singla, "Impact of Selfish Node Concentration in MANETs", International Journal of Wireless & Mobile Networks (IJWMN), vol. 3, no.2, April 2011.
13. T.V.P.Sundararajan & Dr.A.Shanmugam, "Behavior Based Anomaly Detection Technique to Mitigate the Routing Misbehavior in MANET", International Journal of Computer Science and Security (IJCSS), vol. 3, Issue 2.
14. Takahiro Hara, "Effective Replica Allocation in Ad hoc Networks for Improving Data Accessibility," IEEE INFOCOM, 2001.
15. Takahiro Hara, Norishige Murakami and Shojiro Nishio, "Replica Allocation for Correlated Data Items in Ad Hoc Sensor Networks", SIGMOD Record, vol. 33, no.1, March 2004.
16. Takahiro Hara, "Replica Allocation Methods In Adhoc Networks With Data Update", 2003.
17. Usha.S, "Multi Hop Acknowledgement Scheme based Selfish Node Detection in Mobile Ad hoc Networks", International Journal of Computer and Electrical Engineering, Vol. 3, No. 4, August 2011.