TAMING ENACTMENT USING NEIGHBOR DISCOVER DISTANCE AGAINST MASQUERADING ATTACK IN MANET

Shalini.A[1], Arulkumaran.G[2], Srisathya.K.B[2]
[1]PG Scholar, [2]Assistant Professor,
[1,2]Department of Information Technology, Vivekanandha College of Engineering for Women, Tiruchengode, TamilNadu, India.

ABSTRACT

A Mobile ad hoc network is composed of mobile, wireless devices, referred to as nodes that communicate only over a shared broadcast channel. An improvement of such a network is that no fixed infrastructure is required: a network for routing data can be formed from whatever nodes are available. The node forward messages for each other to provide connectivity to nodes outside direct broadcast range. Ad hoc routing protocols are used to discover a path end-to-end through the cooperative network. In the Sybil attack a single node presents multiple fake identities to other nodes in the network. Sybil attacks pose an immense threat to decentralized systems like peer-to-peer networks and geographic routing protocols. In our proposed method we have using passive ad hoc identity method and key distribution. To take throughput, delivery ratio, delay, energy efficient parameters are to be taken for differentiate the results on network. Improve the network overall performance and secure data transmission on the network. We have intend neighbor discover distance method and key distribution methods to ensure the performance against Masquerading Attack.

KEY WORDS- *GRP, Key Distribution, Mobile Ad hoc Network, Masquerading Attack, NDD.*

1. INTRODUCTION

Mobile ad hoc networks (MANET) represent complex distributed systems that consist of Wireless Mobile nodes can dynamically and freely self-organize into arbitrary and temporary ad hoc network topologies.

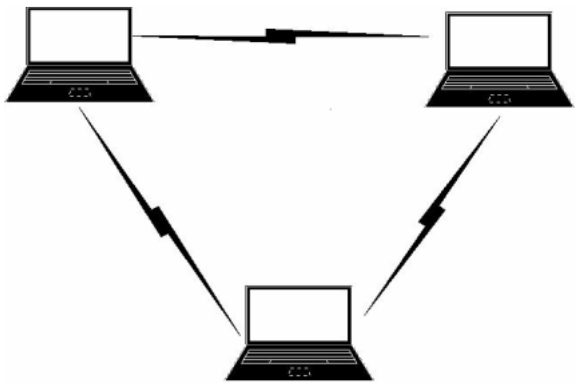

Figure: 1 Structure of Ad hoc Network

The Mobile ad hoc networks (MANET) have attracted a lot of attentions due to their interesting and promising functionalities including mobile safety, traffic congestion avoidance, and location based

services. In this paper, we focus attention on safety driving application, where each node occasionally broadcasts messages including its current position, path and swiftness, in addition to node information. The privacy is an important issue in MANET. As the wireless communication channel is a shared medium and exchanging messages without any security protection over the air can easily leak the information that users may want to keep private. Pseudonym based schemes have been proposed to preserve the location privacy of mobile. However, those schemes require the mobile to store a large number of pseudonyms and certifications, and do not sustain some important secure functionality such as authentication and integrity.

The centralized key management has some disadvantages. For instance, the system maintenance is not flexible. The issue regarding the centralized key management is that many existing schemes assume a tamper-proof device being installed in each vehicle. The tamper- proof device normally cost several thousand dollars. The framework is developed in this paper does not require the expensive tamper-proof device. In this manuscript it is used and develops a secure distributed key management framework.

A. Sybil Attack

Ad hoc network is composed of mobile and wireless devices referred to nodes that communicate only over a shared relay channel. A benefit of such a network is that no fixed infrastructure is required: a network for routing data can be formed from whatever nodes are available. Nodes forward messages for each other to provide connectivity to nodes outside direct broadcast range.

Each node wants a unique address to participate in the routing. IP addresses or unique media access channel (MAC) addresses are assigned in routing. Because all communications are conducted over the broadcast channel, nothing but these identifiers is available to determine what nodes are present in the network. In particular, our scheme utilizes the RSS in order to differentiate between the legitimate and Sybil identities. First it demonstrates the entry and exit behavior of legitimate nodes and Sybil nodes using simulation and test bed experimentation. Second it defines a threshold that distinguish between the legitimate and Sybil identities based on nodes entry and exit behavior. Third it tunes our detection by data fluctuation.

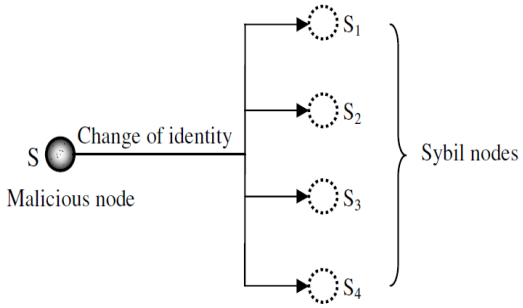

Figure: 2 Creating Multiple Identities

B. Detecting the Sybil Attack

In the mobile environment a single entity impersonating multiple identities has an important constraint that can be detected: because all identities are part of the same physical device, they must move in unison, while independent nodes are free to move at will.

As nodes move geographically all the Sybil identities will appear or disappear as the attacker moves in and out of range simultaneously. It considers an attacker uses a single-channel radio, multiple Sybil identities must transmit serially, whereas multiple independent nodes can transmit in parallel. The identities established by a Sybil attacker whether represented by MAC addresses, IP addresses or public keys differ from those of an honest node in several ways. Because the resources of a single node are used to simulate multiple Identities, resource constrained in computation, storage or bandwidth for particular identities. In existing system they used scheme intrusion detection method to find Sybil Attacks [1].On the other hand its pose some other problems like Masquerading Attacks.

C. Masquerading Attacks

During the neighbor acquisition method, an outside intruder might masquerade a nonexistent or existing IS (Information Systems) by attaching itself to communication link and illegally joining in the routing protocol domain by compromising an authentication system. The threat of masquerading is almost the same as that of a compromised IS.
In this paper we are going to rectify a Masquerading Attack which poses serious Threat in mobile ad hoc network as another form of Sybil Attack. Here it proposes a scheme to NDD and Key Distribution to find a difference between legitimate node and malicious nodes.

2. RELATED WORK

V. PalaniSamy [2] The Security issue of MANETs in group communications because of involvement of multiple senders and multiple receivers is even more challenging. At that time of multicasting, because of vulnerabilities of routing protocols mobile ad hoc network are unprotected by the attacks of malicious nodes. Some of the attacks are Rushing attack, Neighbor attack, Black hole attack, Sybil attack and Jellyfish attack. The goal is to measure the impact of Rushing attack and their node positions by near sender, near receiver and anywhere scenario within the network which affect the performance metrics of Average Attack Success Rate. The performance of the Attack Success Rate with respect to above three scenarios is also compared.
Prof. Doutor Rui Jorge [3**]** project proposes the ad hoc network secure has often to rely on Byzantine fault-tolerance techniques which typically rely on quorum based security protocols. If a single adversary can participate in the network with multiple identities a manner known as the Sybil Attack quorums may be easily overwhelmed. This notion addresses the difficulty of preventing the Sybil Attack in wireless ad hoc networks. In particular, it is proposed an algorithm that allows the correct nodes in a one-hop neighborhood to have a familiar set of non-Sybil identities. The algorithm is based on the combination of several types of resource tests, which were developed from a proportional analysis.
Chris Pire [3] proposes several new defenses against the Sybil attack which including key validation for random key pre distribution, position verification, radio resource testing and registration. The quantitative analysis show the radio resource testing method is very effective given the assumption that a malicious node cannot send on multiple channels simultaneously. It also presents a quantitative evaluation for the random key pre distribution approach showing that it is robust to compromise nodes. It exactly show that in the multi-space pair wise scheme storing 200 keys at each node, the attacker would have to compromise 400 nodes before having even a 5% chance of being able to fabricate new identities for the Sybil attack.

3. EXTENDED APPROACH

In existing system hackers easily can proceed as source node and sends message to destination. The destination receives incorrect message from hackers. Destination believes that its accurate message from source. Destination receives the incorrect information from hackers. The communications are passed from sender to destination (receiver) without any security. Sybil attacks pose a serious threat to such networks. A Sybil attacker can also generate more than one identity on a single physical device in order to launch a coordinated attack on the network or can switch identities in order to weaken the detection process, in this manner promoting lack of accountability in the network. The message header holds source node information which sends the message to receiver. The hackers can easily modify that header information and sends to destination. This has loss of data and not a secure process on the network.

A. Existing Solution

- **Destination gets the wrong information from hackers or malicious user**.
  It blocks legitimate users or hackers by maintaining centralized server.
- **There is no any server to detect hackers**.
  The proposed algorithm create server to detect unauthorized user.
- **Overhead of packet loss**

It Controls an overhead packet loss

- **Low level network performance**
  Passive ad hoc identity involves in improvement of network performance

In this proposed system, one centralized server is maintaining to check authentication of source where hackers cannot act as source. It blocks legitimate users or hackers. It has to afford a key based data transmission and id based network. The passive ad hoc identity similar to Neighbor discover distance (NDD) node to watch the transmission on the network. The proposed system used the NDD Algorithm. Use these algorithms to transfer the data in source to destination without any damage or loss as well as each node to have the neighbor's node address. Depends on the address the data will be transmitted in to accurate destination. If any packet loss or some collisions on network immediately it informs the server to stop the data and maintaining source node information and header information of communication. It verifies the users using those details whether they are attackers or ordinary user. The information of hackers has not been transferred to destination. The destination has not been in receipt of any attacker information. In this proposed manner it uses secure transmission and avoids the attacking system on the network.

B. Neighbors discover distance (NDD) Algorithms

Step 1: Each node to know the neighbors node address.
Step 2: If neighbors node is centralized server node means
Store data
Else
Search the centralized node.
Step 3: The server nodes have all source data as fit as destination address.
Step 4: Each node has the individual keys. It depends on the keys the centralized server is to identify the destination address.
Step 5: The Neighbor Discover Distance algorithm and centralized server method is used to preventing the data in to any attackers
Step 6: The destination node easily to check the data is correct or not.
Step 7: If any attackers damage the data means destinations node again send the data in to centralized server.
Cooperative communication has received tremendous interest for wireless networks. The existing works on accommodating communications are focused on link-level physical layer issues. For that reason network-level upper layer issues the impacts of cooperative communications such as routing topology control and network capacity are largely ignored.

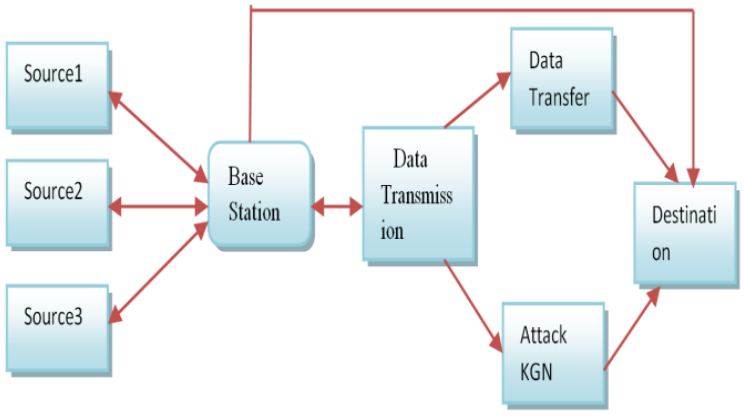

Figure: 3 Proposed Architecture Diagram

Here propose a capacity-optimized cooperative topology control scheme to improve the network capacity in MANET by jointly considering both upper layer network capacity and physical layer cooperative interactions. During simulations, we show that physical layer cooperative communications have significant impacts on the network capacity and the topology control scheme can substantially improve the network capacity in MANETs with cooperative communications. It is to

improve the performance of the topology network so it has using the traffic aware method of the network topology.

4. EXPERIMENTS AND TEST

A. Topology Design

Without using any cables then fully wireless equipment based transmission and received packet data. The node and wireless link is to gauge sending and receiving packets. The sink is present at the center of circular sensing area. It intermediate the sender and receiver of networking performance on this topology.

B. Node Creating

This module is developed to node creation and more than 10 nodes placed particular distance. The wireless node placed at intermediate area to watch transmission of packet. The access point has to receive transmit packets then send acknowledge to transmitter.

C. Network Simulator2

After setting up the platform, software named NS2 was set up on it which was used for all the analysis and simulation work apart from further tools used. The NS2 is the de facto standard for network simulation. The behavior is vastly trusted within the networking area. ISI, California urbanized it and is supported by the DARPA and NSF. An object oriented simulator NS2, written in C++, with an OTcl interpreter as a frontend. This is for the huge part of the simulation scripts are created in Tcl. If the components have to be developed for NS2, then both Tcl and C++ have to be used. NS2 uses two languages because any network simulator has two different kinds of effects it needs to do. The one hand complete simulations of protocols require a systems programming language which can efficiently manipulate packet headers and perform algorithms that run over huge data sets. For these tasks the run-time speed is essential and turn-around time (run simulation, find bug, fix bug, recompile, re-run) is less important. The other hand a huge part of network research involves slightly varying parameters or configurations are promptly exploring a number of scenarios. In these cases iteration moment (change the model and re-run) is more important. The configuration runs once (at the beginning of the simulation) run-time of this ingredient of the task is less important.

D. Throughput

It is dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation that is the information about whether or not data packets correctly delivered to the destinations.

E. Graph Design Based Result

Graph is a fundamental ingredient of display a result, so we plot a graph to show a various result comparison with packets, throughput, delivery ratio, network delay, energy efficient and etc.

F. Results

The simulation is done with multiple nodes in connection and analysis the network performance from the attacks.

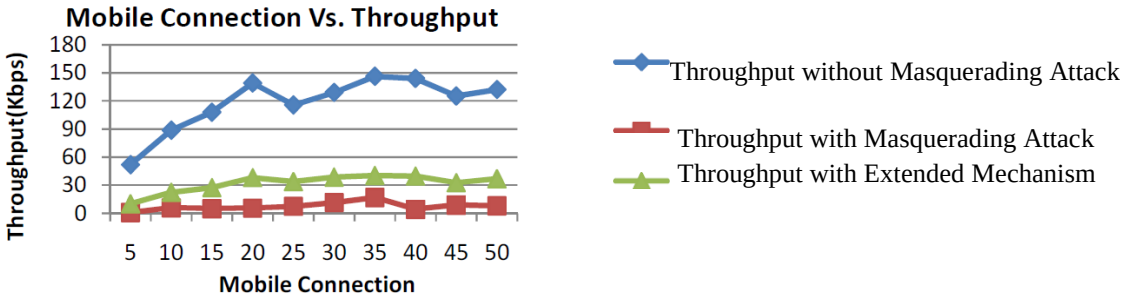

Figure: 3 Show Throughputs

The Figure 3 shows the graph of performance and throughput when a mobile node varies in connection. The Proposed mechanism is used in the presence of Masquerading Attacks.

5. CONCLUSION

In this paper we propose a Neighbor Discover Distance Algorithm to safeguard the network against Masquerading Attacks. We demonstrated through various simulations for the distinction of legitimate nodes and malicious nodes identities. This proposed system also shows the various factors which affect network performance Packet Transmission Rate and nodes Speeds. Our Scheme shows the results works better in mobile environments and detects attackers with high degree of accuracy in the network.

REFERENCES

[1] Sohail Abbas, Madjid Merabti, David Llewellyn-Jones, and Kashif Kifayat," Lightweight Sybil Attack Detection in MANETs", IEEE Systems Journal, Vol. 7, No. 2, June 2013.
[2] V. Palanisamy1, P.Annadurai2,," Impact of Rushing attack on Multicast in Mobile Ad Hoc Network"**,** (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.
[3] C.Piro, C. Shields, and B. N. Levine, "Detecting the Sybil attack in mobile ad hoc networks," in Proc. Securecomm Workshops, 2006, pp. 1–11.
[4] B. Xiao, B. Yu, and C. GAO, "Detection and localization of Sybil nodes in VANETs," presented at the Proc. 2006 Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks, 2006, pp. 1–8.
[5] V. Frias-Martinez, S. J. Stolfo, and A. D. Keromytis, "BARTER: Behavior profile exchange for behavior-based admission and access control in MANETs," presented at the Proc. 5th Int. Conf. Information Systems Security, Kolkata, India, 2009, pp. 193–207.
[6] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. "Detecting Black hole Attack on AODV based Mobile Ad hoc Networks by Dynamic Learning Method". International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov 2007.
[7]Yingying Chen, Jie Yang, Wade Trappe and Richard P. Martin, Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks," IEEE Transactions on Vehicular Technology, Vol. 59, No. 5, June 2010.
[8] Yu, H., M. Kaminsky, P. Gibbons, & A. Flaxman (2008)," Sybil guard: Defending against Sybil Attacks via Social Networks", Networking, IEEE/ACM Transactions on 16 (3), 576–589.
[9] Jayashree.A.Patil and Nandini Sidnal, Ph.D.," Survey - Secure Routing Protocols of MANET**",** International Journal of Applied Information Systems (Ijais) – ISSN: 2249-0868, March 2013.
[10] Ziming Zhao and Hongxin Hu, "Risk-Aware mitigation for MANET Routing Attacks", IEEE transactions on dependable and Secure Computing, Vol. 9, No. 2, March/April 2012.
[11] Maha Albelhah and Rosilah Hassan, "Detecting Sleep Deprivation Attack over MANET Using a Danger Thoery-Based Algorithm", International Journal on New Computer Architecture Ant Their Application (IJNCAA)-2011.