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. 8, August 2014, pg.713 – 719

RESEARCH ARTICLE

Verification and Innovation of Neighbor Positions in MANETs

A. Yuvaraj[1], Manohar. K[2]

[1]M.Tech 2nd year, Department of CSE, ASCET**,** Gudur, A.P, India

[2]Associate Professor, Department of CSE, ASCET, Gudur, A.P, India

[1] yuvaraj8099@gmail.com; [2] gmanoharkp@gmail.com

Abstract- In this paper generally MANETs are self-configuring autonomous networks that do not need any central authority to control and coordinate the network. In this neighborhood discovery (ND) is the process of discovering the devices that are directly reachable for communication or in physical proximity. So it becomes a fundamental requirement and building block for various other applications. It is very easy to abuse ND and there by compromise the overlying protocols and applications. Thus, providing methods to mitigate this vulnerability and secure ND is essential. This paper uses the directional antenna algorithm called as scanning based direct discovery algorithm to discover the neighbors, and location awareness is an important asset in mobile systems and many protocols require knowledge of position of the participating nodes. To allow cooperative working of the variety of distributed protocols we use trust system to provide the trust level of various nodes, thereby enhancing the cooperation amongst the nodes. This paper uses distributed hybrid trust algorithm and as well uses relationship maturity concept to compute the trust of the nodes. This paper demonstrates that Trust systems are better than already existing cryptographic techniques.

Keywords- Neighbor position verification protocol, mobile ad-hoc networks, Spontaneous network, Neighbor discovery, Relationship maturity, Trust

I. INTRODUCTION

Mobile Ad hoc networks are wireless networks with no fixed infrastructure in which nodes depend on each other to keep the network connected. A mobile ad hoc network (**MANETs**) is a self-configuring infrastructure-less network of mobile devices connected by wireless. It consists of a collection of mobile hosts that may communicate with each another from moment in time to time. In this no base stations are supported. In this Mobile Ad-Hoc Networks, Routes may be disconnected due to dynamic movement of nodes. Due to mobility in MANETs, each device is free to move independently in any direction, and will for that reason change its links to other devices regularly. Here each device must forward traffic distinct to its own use, along with therefore be a router. In this the primary challenge in construction of a MANET is

equipping each device to continuously maintain the information required to accurately direct the traffic. Most traditional mobile ad hoc network routing protocols are designed focusing on the efficiency and performance of the networks.

Location awareness is becoming a significant capability for mobile computing devices, where many protocols need knowledge of the position of the participating nodes. For example, knowledge about neighboring nodes can be used to route, cluster and broadcast in an efficient manner. Whenever a node needs to send data to another node on a network, it must first know where to send it. If the node cannot directly connect to the destination node, it has to send it via other nodes along a proper route to the destination node. Geographic routing in spontaneous networks, data gathering in sensor networks, movement coordination among autonomous robotic nodes, location-specific services for handheld devices, and danger warning or traffic monitoring in vehicular networks are all examples of services that build on the availability of neighbor position information. Here, the challenge is to perform, in absence of priori trusted nodes, a fully distributed, lightweight NPV procedure that enables each node to attain the locations advertised by its neighbors, and evaluate their honesty.

An NPV protocol having the following features:

- NPV protocol is designed for spontaneous ad hoc environments, and it does not depend on the presence of a trusted infrastructure or of a priori trustworthy nodes.
- NPV gears the node to perform all verification procedures autonomously.
- NPV protocol is reactive, (i.e.) it can be executed by any node, at any point in time, without prior knowledge of the neighborhood.
- It is hard against independent and colluding adversaries.
- NPV is lightweight protocol, and it generates small overhead traffic.

➢ *NPV protocol*

The NPV protocol is used to exchange the messages and verifies the position of communicating nodes. In this Protocol, four set of messages are exchanged. They are…

- POLL message
- REPLY message
- REVEAL message
- REPORT message

➢ *POLL message*

In this assumes A is verifier S initiates this message. This message is anonymous. The verifier identity is kept hidden. Here software generated MAC addresses is used. This carries a public key K'S chosen from a pool of onetime use keys of S'.

➢ *REPLY message*

In reply message A is communication neighbor X receiving the POLL message will broadcast REPLY message after a time interval with a freshly generated MAC address. This also internally saves the transmission time. It contains some encrypted message with S public key (K'S). This message is called as commitment of X CX.

➢ *REVEAL message*

The REVEAL message broadcasting is completed by using Verifier's real MAC address. It contains a map MS, a proof that S is only the author of the original POLL and the verifier identity, i.e., its certified public key and signature.

➢ *REPORT message*

In this The REPORT carries X's position, the transmission time of X's REPLY, and the list of pairs of reception times and temporary identifiers referring to the REPLY broadcasts X received. The identifiers are obtained from the map MS incorporated in the REVEAL message. And Also, X discloses its own identity by including in the message its digital signature and certified public key.

II. RELATED WORK

In this paper the most important requirement of the ad-hoc networks is that they are "self-configuring" i.e., that a large number of wireless nodes arrange themselves to efficiently perform the tasks required by the application later than they have been deployed.

After nodes are deployed, they do not have knowledge about the neighbors thus, they need to determine their neighbors in order to communicate with them. Knowledge of the neighbors is essential intended for almost all routing protocols, medium-

access control protocols and several other topology-control algorithms. Neighbor discovery (ND) is, therefore, a crucial first step in the process of self-organization of a wireless ad-hoc network.

The neighbors can be either physical neighbors or communication neighbor [8]. The physical neighbors are those that are in the range of physical proximity of the discoverer. The communication neighbors are those that are available for communication but need not to be in the physical range of the discoverer [7].

The types of neighbor discovery algorithms are direct discovery algorithm or gossip based algorithm. The various other parameters are used to classify the discovery algorithms are known or unknown number of neighbors, synchronous or asynchronous nodes in network [1]. In this we use direct discovery algorithm to discover the physical neighbors.

Since almost all the protocols deployed in the Ad hoc networks are distributed, cooperation among the nodes is very essential. So to ensure the cooperation among nodes, the network should not contain any malicious nodes. We use trust management system to predict the trust level of the node. And Trust metric is useful not only to identify the malicious node but also when the nodes exchange information with each other.

In this journal paper we use distributed trust (i.e.) every node will calculate the trust level of every other node. The centralized trust systems require a centralized trust agent to calculate the trust level of every node in the system. But this system may be compromised completely if the trust agent is compromised.

The proposed method uses both direct trust computation as well as receive recommendations from the neighbors. The concept of relationship maturity [6] is used in the proposed model to provide weights for the recommendations received from the neighbors. In this the recommendations from neighbors who are known for longer period of time will be given more weight than those from the newer neighbors. This might reduce the probability of false recommendations.

The proposed model uses neural network which has the ability to learn by itself, and to implement the trust systems. The neural networks have the ability to build more flexible and dynamic trust systems that can be retrained to frustrate a multitude of attack patterns simply and efficiently.

In randomized neighbor discovery [1], each node transmits at randomly chosen times and discovers all its neighbors by a given time with high probability.

In deterministic neighbor discovery [1], on the further hand, each and every node transmits according to a predetermined transmission schedule so as to allow it to determine all its neighbors by a given time with probability.

The antenna models are used in ad hoc networks are Omni directional antenna model or directional antenna methods come. The Omni directional antenna method [10] propagates signal in all directions. The algorithm used by Omni directional antenna is 1-way algorithm where the receiver will not send any acknowledgement after receiving the discovery message. The sender broadcasts the DISCOVER message to advertise itself. The receivers will discover one neighbor if it receive the DISCOVER message correctly in the listen state.

The Omni directional antennas have drawbacks like reduced gain, high bandwidth consumption, increased noise and increased signal distraction.

Directional antennas provide longer transmission range and higher data rate. They strongly reduce signal interferences in unnecessary directions and reduce jamming susceptibility.

The directional antenna algorithms used to discover neighbors. The radiation pattern of directional antenna is shown in figure 1.

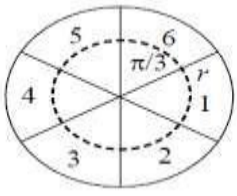

Figure 1 Radiation pattern of directional antenna

In direct discovery algorithm [9] the nodes determine the neighbors which communicate with it directly. The method used to discover the neighbors is recording the angle of arrival of the beacon signal, determining the location based using GPS. The direct discovery algorithm will discover only those neighbors that communicate with it straight.

In gossip based algorithm [9] the neighbors are discovered indirectly through the interaction with other neighbors. Messages are exchanged to discover the neighbors. The message consists of the list of neighbors‟ IDs and their locations. The main drawbacks of gossip based algorithm are message length grows as more and more nodes are discovered and the presence

of physical obstacles can cause nodes to incorrectly infer another node as its neighbor.

The Direct Symmetry Test and Cross Symmetry Test was proposed in [5] is used to verify the location of the neighbors that the nodes are declared.

III. Trust Method

Trust is an important aspect of mobile ad hoc networks (MANETs). It enables entities to manage with uncertainty and uncontrollability caused by the free will of others. Trust model is very important in the distributed collaborative environment. Collaborations and information sharing are measured to be essential operations in the MANET to achieve the deployment goals such as sensing and event monitoring. Collaboration will be productive only if all participants operate in a trustworthy manner.

MANETs are usually deployed in harsh or uncontrolled environments, thereby heightening the probability of compromises and malfunctioning as there is no central control unit to monitor the node operations. Here these characteristics force a component node to be cautious when collaborating / communicating with other nodes as the behavior of nodes change with time and environmental conditions. For that reason, establishing and quantifying behavior of nodes in the form of trust is necessary for ensuring proper operation of MANET.

Trust computations consist of three components: They are „experience", „recommendation" and „knowledge". The „experience" component of trust for every node is directly measured by their immediate neighbors and kept updated at regular intervals in the trust table. The existing trust table is propagated to all other nodes as „recommendation" part of the trust. At a regular interval, the previously evaluated trust is included in the current „knowledge" component of total trust.

The work on trust computations can be broadly classified into the following categories [4]: They are…

- ***Distributed trust computations***: Every node computes its own value of trust on its neighbors.
- ***Centralized trust computations***: central agent manages/helps the node in trust computations.
- ***Hybrid trust computation***: In Hybrid trust on a node is computed based on direct experience and also recommendations from other nodes.

The Bayesian Approach used in [3] varies the weights for information according to their occurrence time and providers. It uses exponential decrease method to expire the old observations.

The trust model proposed in [2] contains two modules namely, Monitoring Module (MM) and Reputation Handling Module (RM). The MM monitors the packet forwarding activities of the node and the RM is responsible for managing the reputation information.

IV. Verification of Neighbor Positions

The overall flow of the system is shown in the following figure, the positioning of neighbors is completed and the nodes are classified. Afterward these positions that are claimed are verified. In this the new nodes are updated when they enters or leaves the range. Here the same verification processes are done while updating [11].

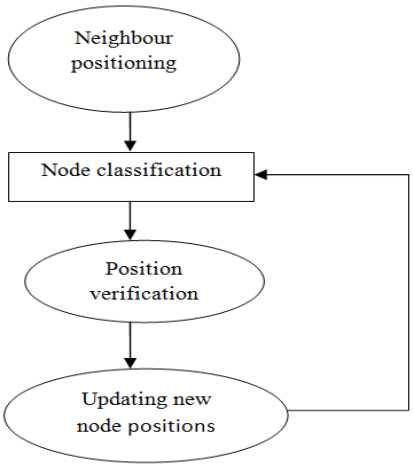

Fig: system flow

Adversaries can be internal or external. Adversaries equipped with cryptographic keys and credentials that allow them to participate in the execution of the VC system protocols are termed as internal adversaries. In this Adversaries that do not possess keys and credentials are external adversaries. [12]

A single independent adversary cannot perform any successful attack against NPV scheme. Only multiple independent adversaries can harm each other, thus reducing their probability of successfully announcing a false position. In this to rectify this problem, a new protocol is introduced namely, Spontaneous Wireless Ad Hoc Network protocol". Later than identifying the position and verifying its neighbor, the next step is to exchange the information with its neighbors in a make safe manner by using the spontaneous wireless ad hoc network protocol.

- *System implementation*

In this System implementation the initial step in the setting up the Ad Hoc networks is the neighbor discovery. After that discovering the neighbors the system will monitor the neighbor nodes by capturing the network packets. In this the neural network is trained with the past historical data and as well as the weights are adjusted accordingly to get the desired output. Then the gathered packet associated information is fed to the trained neural network to compute the trust value.

Then the recommendations about the selected node by the neighboring nodes are collected. Then the aggregated trust is formulated by summing up the direct trust value and the recommendations. The recommendations are weighted based on the relationship maturity.

Here Next step is to update the trust value of a node in the trust record by comparing the existing trust value with the defined threshold value. But if the trust level of the node is lower than the threshold value then the trustworthiness of the node is said to be untrusting as well it is set as trust worthy node.

- *Discovery of neighbor nodes*

The algorithm used in the proposed model for ND is Scan based Random algorithm for neighbor discovery. The scam based algorithm used in the proposed system is completely random algorithm (CRA). In this the CRA does not have the prior knowledge of how many number of nodes are there in the network.

The CRA used in the proposed system is the direct discovery algorithm that uses the directional antenna for transmission and reception of signals. In this the algorithm requires the nodes to that communicate to be synchronized. It can successfully transmit and receive only if the nodes are in complementary mode.

The algorithm divides the time frame into three slots. During the first mini slot the node decides to be in every one of the following state. The states of node are described as follows….

- Transmit
- Listen
- Sleep

In this Weight of the recommendations coming from older neighbors and decreases the weight of recommendations coming from new neighbors. Here the trust computation formula used in the proposed system is as follows:

$T_A(B) = Q_A(B) + R(B)$ (1) Where $T_A(B)$ is trust computed by A about B, $Q_A(B)$ Represents the direct trust compute by about B, R(B) is the aggregated recommendations about node B by all its neighbors.

The direct trust is computed by monitoring the network nodes using packet analyzers. The analyzer captures the packets of the neighbor nodes in the promiscuous mode and extracts the information required for trust computation. This information is fed to a trained neural network to compute the trust of the neighbor nodes.

The recommendations about the neighbors are received sing REP (Recommendation exchange protocol). REP is used to exchange the trust related information only between the neighbors. The recommendations are not forwarded throughout the network.

- *Trust Algorithm*

Trust algorithm is used for computing the trust of the neighbor nodes in the proposed system is relationship maturity based distributed trust management scheme. This algorithm used in the proposed model is distributed where each node computes the trust of every other node. It uses both direct trust and as well as recommendation based trust for computing the trust.

To perform the weight age of the recommendation the proposed system uses the relationship maturity concept where the age of relationship is measured. The Nodes increase the weight of the recommendations coming from older neighbors and decrease the weight of recommendations coming from new neighbors. The trust computation formula used in the proposed system is as follows:

$$TA(B) = QA(B) + R(B) \quad (1)$$

Where TA (B) is trust computed by A about B, QA (B) represents the direct trust compute by about B, R (B) is the aggregated recommendations concerning node B by all its neighbors. In this the direct trust is computed by monitoring the network nodes using packet analyzers. The analyzer captures the packets of the neighbor nodes in the promiscuous mode and extracts the information required for trust computation. This information is feed to a trained neural network to compute the trust of the neighbor nodes. The recommendations about the neighbors are received sing REP (Recommendation exchange protocol). REP is used to exchange the trust related information only among the neighbors. The recommendations are not forwarded throughout the network.

V. CONCLUSION

The algorithms are used to discover the neighbor nodes that are used in the existing model are Omni directional antenna based algorithm, directional antenna based algorithm and gossip based algorithm. These algorithms are useful to identify the neighbors but these algorithms do not provide the security architecture to identify the malicious or misbehaving nodes.

In this paper mainly we integrate the trust based security system to the neighbor discovery process, in order to recognize the malicious and selfishly behaving nodes. The proposed system aims to reduce the number of time slots needed to discover all the neighbors in the network and also it provides security mechanism to improve the cooperation among the neighbor nodes. The trust among the neighbors is established to enhance the collaborative work among the neighbors. The proposed system exchanges the trust information about the nodes only with their neighbors thus it reduces the number of messages forwarded into the network and the data traffic in the network.

REFERENCES

[1] Sudarshan Vasudevan, Micah Adler, Dennis Goeckel, Fellow, IEEE, and Don Towsley, Fellow, IEEE, ACM "Efficient Algorithms for Neighbor Discovery in Wireless Networks".

[2] Jaydip Sen, "A Distributed Trust and Reputation Framework for Mobile Ad Hoc Networks" Jie Li and Ruidong Li, University of Tsukuba, Jien Kato, Nagoya University, " Future Trust Management Framework for Mobile Ad Hoc Networks ",0163-6804/08/ 2008 , IEEE Communications Magazine ,2008

[3] Kannan Govindan, Member IEEE and Prasant Mohapatra, Fellow IEEE, " Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey "

[4] Marco Fiore, Member, IEEE, Claudio Casetti, Member, IEEE, Carla-Fabiana Chiasserini, Senior Member, IEEE,Panagiotis Papadimitratos, Member, IEEE , "Discovery and Verification of Neighbor Positions in Mobile Ad Hoc Networks"

[5] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle, " Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model ".

[6] Reza Azmi, Mahdieh Hakimi, and Zahra Bahmani , "Dynamic Reputation Based Trust Management Using Neural Network Approach", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 1, September 2011

[7] Panos Papadimitratos and Marcin Poturalski,, "Secure Neighbor Discovery: A Fundamental Element for Mobile Ad Hoc Networks" ,IEEE Communication Magazine, 2008.

[8] Panos Papadimitratos and Marcin Poturalski,, "Secure Neighbor Discovery: A Fundamental Element for Mobile Ad Hoc Networks" ,IEEE Communication Magazine, 2008.

[9] Sudarsan Vasudevan, Jim Kurose, Don Towsley, "On Neighbor Discovery in Wireless Networks with

Directional Antennas", UMass Computer Science Technical Report 04-53 ECC-0313747001.

[10] Zhensheng Zhang and Bo Li, "Neighbor Discovery in Mobile Ad Hoc Self-Configuring Networks with Directional Antennas: Algorithms and Comparisons".

[11] P.Papadimitratos, M.Poturalski, P.Lafourcade, D.Basin, S.Capkum, and J-P,Hubaux, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad-Hod Networks," IEEE comm.Magazine,vol.46,no.2,pp.132- 39,Feb.2008.

[12] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P.Hubaux, "Secure Vehicular Communications: Design and Architecture," IEEE Comm. Magazine, vol. 46, no. 11, pp. 100-109, Nov. 2008.

