ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 9, September 2016

Trust based Secure Graph Detection Algorithm with Routing Graph Modelling in Wireless AdHoc Network

S.Vishnupriya[1] , Dr. P.Senthilvadivu[2]

M.Phil Research Scholar, Hindusthan College of Arts and Science, Coimbatore, India[1]

Associate Professor & Head, Department of BCA, Hindusthan College of Arts and Science, Coimbatore, India[2]

ABSTRACT: Secure Routing is a fundamental networking function in all communication system, and multi-hop wireless networks are no exceptions. Attacking the routing service, an adversary can easily paralyze the operation of an entire network. In this paper, proposed a Trust based secure graph detection algorithm (TSGD) will improve the Dynamic Networks with Probabilistic Graph Modeling with Authenticated secret Secure Routing for MANETs to reduce the connectivity and packet delay of hosts. A possible method is to combine it with a trust based routing. With the help of the trust model, the routing protocols will be more active in detecting link failures, caused either by the mobility or adversary attacks. Through extensive simulations and verification proposed mechanism achieves significantly better detection accuracy than conventional methods such as a routing protocol strategy based detection.

KEYWORDS: Secure routing; Manets; Mobility model; PDR; CBR

I. Introduction

Mobile Ad hoc Network (MANET) is a collection of mobile devices (called nodes) that communicate with each other without the use of infrastructure such as access points or base stations. These self-configuring networks are capable of self-directed operations and can be deployed easily. They are also referred to as Self-Organizing Networks (SON), in which the nodes cooperate among themselves to provide connectivity and operate without centralized administration [1]. MANETs are used in a variety of applications, such as, vehicular ad hoc networks (VANET), sensor networks, military networks, robotic mobile networks, etc.

Many security schemes from different aspects of MANET have been proposed in order to protect the routing information or data packets during communications, such as secure routing protocols and secure key management solutions. Due to resource scarcity (battery power, memory, and processing power) of nodes, securing MANET is quite different from traditional schemes that generally involve management and safe keeping of a small number of private and public keys. The security mechanism for MANET, on one hand, must require low computation complexity and a small number of appended messages to save the node energy. On the other hand, it should also be competitive and effective in preventing misbehaviors or identifying misbehaving nodes from normal ones. However, most of these schemes assume that there are trusted third parties or centralized servers who are responsible for issuing digital certificates and keys or monitoring the behaviors of other nodes. Centralized servers or trusted parties make the network more controllable but they destroy the self organizing nature of MANET and reduce the network scalability. Even some schemes distribute the servers into many nodes; there are still bottlenecks due to centralization. If the scheme distributes the functions of servers into each node of the network, it will introduce significant performance overhead. What's more, by requiring nodes to generate and verify digital signatures all the time, these solutions often bring huge computation overhead [3] and [4] and [5]. Therefore, we need a self-organized light-weight security scheme for mobile ad hoc networks.

Large organizations need rigorous security tools for analyzing potential vulnerabilities in their networks. However, managing large-scale networks with complex configurations is technically challenging. For example, organizational networks are usually dynamic with frequent configuration changes. These changes may include changes in the availability and connectivity of hosts and other devices, and services added to or removed from the network.

II. RELATED WORK

In [6] authors proposed a robust and distributed access control mechanism based on a trust model to secure the network and stimulate cooperation by excluding misbehaving nodes from the network. The mechanism divides the access control responsibility into two contexts: local and global. The local context responsibility is the neighborhood watch to notify the global context about suspicious behavior. In its turn, the global context analyzes the received information and decides whether it punishes the suspicious node using a voting scheme. To model the exclusion mechanism and perform a parameter analysis. In [7] authors presented Adhoc On Demand Distance Vector Routing (AODV), a novel algorithm for the operation of such adhoc networks. Each Mobile Host operates as a specialized router, and routes are obtained as needed (i.e., ondemand) with little or no reliance on periodic advertisements. Our new routing algorithm is quite suitable for a dynamic self starting network, as required by users wishing to utilize adhoc networks. In [8] authors presented iterative algorithms to find source and relay beam formers jointly based on alternating optimization. Furthermore, they conduct asymptotic analysis on the maximum secrecy sum-rate. They showed that when all transmit powers approach infinity, the two-phase two-way relay scheme achieves the maximum secrecy sum rate if the source beam formers are designed such that the received signals at the relay align in the same direction. This reveals an important advantage of signal alignment technique in against eavesdropping. In [9] authors explored the physical-layer security in cooperative wireless networks with multiple relays where both amplify-and-forward (AF) and decode-and-forward (DF) protocols are considered. To propose the AF and DF based optimal relay selection (i.e., AFbORS and DFbORS) schemes to improve the wireless security against eavesdropping attack. In [10] authors discussed the secure transmission of information in wireless networks without knowledge of eavesdropper channels or locations is considered. Two key mechanisms are employed: artificial noise generation from system nodes other than the transmitter and receiver, and a form of multi-user diversity that allows message reception in the presence of the artificial noise. To determine the maximum number of independently-operating and uniformly distributed eavesdroppers that can be present while the desired secrecy is achieved with high probability in the limit of a large number of system nodes. While the main motivation is considering eavesdroppers of unknown location, first is to consider the case where the path-loss is identical between all pairs of nodes.

III. PROPOSED ALGORITHM

A. *NETWORK CONSTRUCTION*

The network simulations are evaluated in networks of N number of nodes. As the number of nodes in the ad hoc network is increased, the dimension of the simulation area is also increased so that a consistent node density is maintained. The simulation areas are 1451m x 1000m, and 1000m x1000m, respectively. All mobile nodes move according to the map-based mobility waypoint model. Node speeds are randomly distributed between zero and some maximum, where the maximum speed varies between 0 and 20 m/s. The pause time is consistently 10 seconds. Each data point represents an average of 10 runs with the same traffic models, but different randomly generated mobility scenarios. The second set of simulations examines the performance of the two routing schemes with different percentages of Internet (wired) traffic. Random traffic connections of TCP and CBR can be setup between mobile nodes using a traffic-scenario generator script. It can be used to create CBR and TCP traffics connections between wireless mobile nodes. In order to create a traffic-connection file, we need to define the type of traffic connection (CBR or TCP), the number of nodes and maximum number of connections to be setup between them, a random seed and in-case of CBR connections, a rate whose inverse value is used to compute the interval time between the CBR packets. Directives for GOD are present as well in node-movement. The General Operations Director (GOD) object is used to store global information about the state of the environment, network, or nodes that an omniscent observer.

B. *ROUTING MOBILITY MODEL*

A routing mobility model that forces Mobile Nodes (*MN*) to travel to the edge of the simulation area before changing direction and speed. This model does not suffer from the density waves in the centre of the simulation space that Random Waypoint model does. In this model, MNs choose a random direction in which to travel similar to the Random Walk Mobility Model. An *MN* then travels to the border of the simulation area in that direction. Once the simulation boundary is reached, the *MN* pauses for a specified time, chooses another angular direction (between 0 and 180 degrees) and continues the process.

Movement models govern the way nodes move in simulation. They provide coordinates, speeds and pause times for the nodes.

There are various movement models presented in DTNs. Some of them are discussed here.

- Random Waypoint
- Shortest Path Movement
- Map Based Movement Model

C. *SECURE PROBABILISTIC GRAPH TOPOLOGY*

The secure probabilistic graph topology (SPGT) is basic functionality is to discover adjacencies and disseminate both topology and name prefix information. Such functionality may appear to be straight-forward to design and implement. However, because SPGT uses data networking (DN) Interest and Data packets to propagate routing updates, the design must shift away from the familiar concepts of pushing packets to given network addresses (i.e., any node can send any packet to any other node). Instead, one must think in terms of data names and data retrieval. More specifically, to need a systematic naming scheme for routers and routing updates. It also need to retrieve routing updates promptly without a priori knowledge of when an update may be generated, since a topology or name prefix change can happen any time.

D. *TRUST BASED SECURE ROUTING PROTOCOL*

The trust based Secure Routing Protocol (TSR) was the first Hybrid routing protocol. It was proposed to reduce the control overhead of Proactive routing protocol and to decrease the latency of Reactive routing protocol. It is suitable for the networks with large span and diverse mobility patterns. For each node a routing zone is defined separately. Within the routing zone, routes are available immediately but for outside the zone, TSR employs route discovery procedure. For each node, a separate routing zone is defined. The routing zones of neighbouring nodes overlap with each other's zone. Each routing zone has a radius ρ expressed in hops. The zone includes the nodes whose distance from the source node is at most ρ hops.

IV. PSEUDO CODE

Step 1: A source node needs a route to destination the protocol starts route discovery. During route discovery, source node broadcast RREQ packets through neighboring nodes.

Step 2: While receiving the RREQ packet each node update their routing table

Step 3: Compare both Neighbor List (NL) and calculate the number of common neighbor nodes (common_node) present between sources to destination

```
For i=0;i<number_of_source_neighbors;i++
For j=0;j< number_of_destination_neighbors;j++
        If (NLS(i) =NLD(J))
        Common _node++;
```

Step 4: Initialize one hop neighbors can reach target node with maximum of 3 hop and minimum of 1 hop. If maximum target_hop_count exceeds 3 then target node and their previous hop may be the attacker node.

Step 5: If target_node_count > node_count_thresh then declare the target node and their previous hop nodes are attacker nodes.

Step 6: Send attacker announcement message to all nodes.

Step 7: Any node receives attacks announcement message it removes attacker node id from its neighbor table and Routing Table.

DOI: 10.15680/IJIRCCE.2016. 0409182

V. SIMULATION RESULTS

The proposed simulation accepts the simulation parameters as input which contains the NS2.34 simulation where the novel Trust based secure graph detection algorithm is applied to the mobile adhoc network. Packet delivery Ratio (PDR): the ratio of the data packets delivered to the destinations to those generated by the Constant Bit Rate (CBR) sources. The EPDR shows how successful a protocol performs delivering packets from source to destination. The higher for the value give use the better results. This metric characterizes both the completeness and correctness of the routing protocol also reliability of routing protocol by giving its effectiveness.

PDR is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source mobile node. It can be evaluated in terms of percentage (%). This parameter is also called “success rate of the protocols”, and is described as follows:

$$\boldsymbol{PDR} = \left(\frac{\boldsymbol{Send\ Packet\ no}}{\boldsymbol{Receive\ packet\ no}}\right) \times \mathbf{100} \qquad \boldsymbol{eq}.\,(\mathbf{1})$$

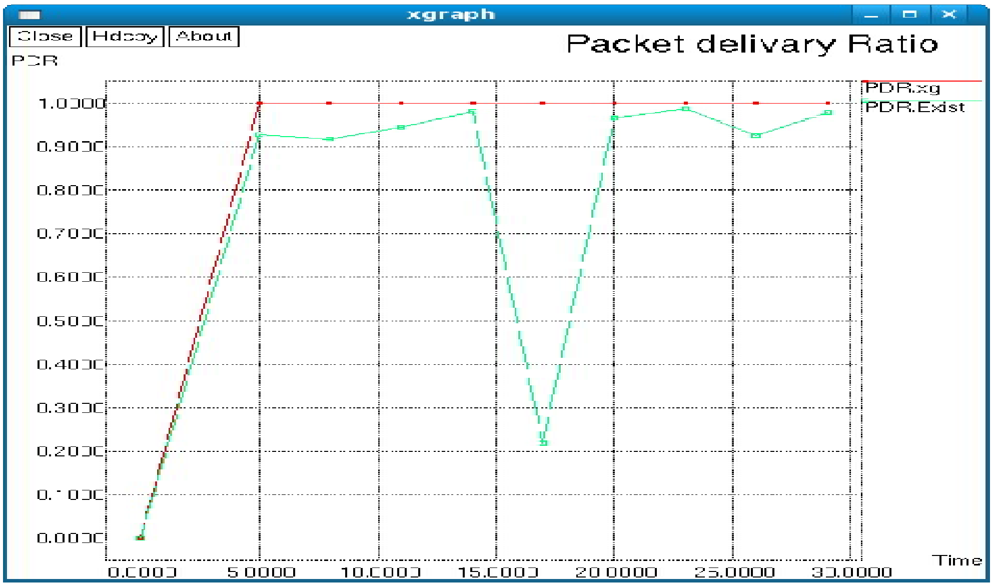

Fig.1. Packet delivery Ratio (PDR)

Data Packet Drop (Packet Loss): Mobility-related packet loss may occur at both the network layer and the MAC layer. Here packet loss concentrates for network layer. When a packet arrives at the network layer. The routing protocol forwards the packet if a valid route to the destination is known. Otherwise, the packet is buffered until a route is available. A packet is dropped in two cases: the buffer is full when the packet needs to be buffered and the time that the packet has been buffered exceeds the limit.

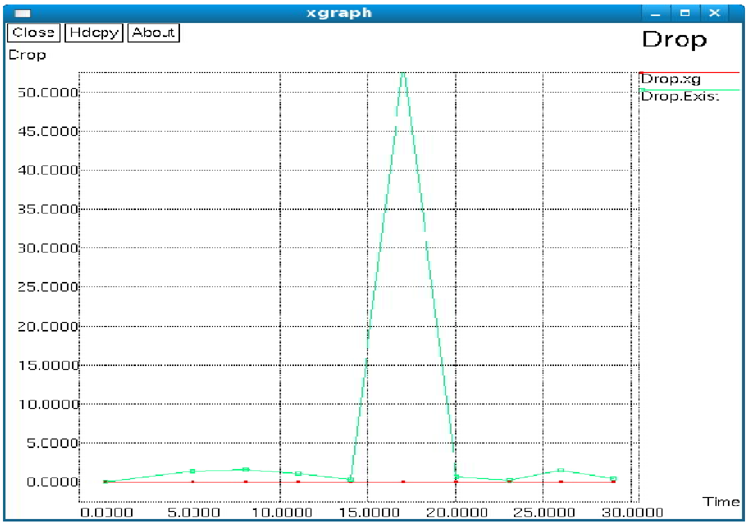

Fig. 2. Data Packet Drop (Packet Loss)

VI. CONCLUSION AND FUTURE WORK

The NS 2.34 simulation results showed that the proposed algorithm Trust based secure graph detection algorithm to solve the problem of secure routing, shortest path selection and packet detection accuracy. The main protocol implemented in this application was the Trust based secure graph detection algorithm (TSGD) protocol, which consists of two important mechanisms, Hybrid routing protocol and path selection routing. Since the TSGG protocol operates exclusively based on source routing and on-demand process, it has been selected as the routing protocol to be implemented and tested for our ad hoc messenger application characterized by a source on-demand chat conversation between nodes in a mobile ad hoc network. The future work can test performance of other routing protocols, such as AODV, DSDV, DSR, geographical forwarding, etc. To compare against the TSGD protocol.

REFERENCES

1. M. Ilyas, The handbook of ad hoc wireless networks. Boca Raton: CRC Press, 2003.
2. D. Wang and P. Wang, "Understanding Security Failures of Two-Factor Authentication Schemes For Real-Time Applications In Hierarchical Wireless Sensor Networks," Ad Hoc Networks - Elsevier B.V., vol. 20 pp. 1–15, 2014.
3. Dalip Kamboj and Pankaj Kumar Sehgal, “A Comparative Study of various Secure Routing Protocols based on AODV”, International Journal of Advanced Computer Science and Applications,Vol. 2, No. 7, 2011, pp 80-85.
4. G.S. Mamatha and Dr. S. C. Sharma, “A Highly Secured Approach against Attacks in”, International Journal of Computer Theory and Engineering, Vol. 2, No. 5, October, 2010, pp 815-819.
5. Mohd Anuar Jaafar and Zuriati Ahmad Zukarnain, “Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment”, European Journal of Scientific Research ISSN 1450-216X Vol.32 No.3 (2009), pp.430-443.
6. L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An Accurate and Precise Malicious Node Exclusion Mechanism For Ad Hoc Networks," Ad Hoc Networks - Elsevier B.V., vol. 19, pp. 142–155, 2014.
7. C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," 2070-1721, 2003.
8. J. Mo, M. Tao, Y. Liu, and R. Wang, “Secure beamforming for mimo two-way communications with an untrusted relay,” IEEE Trans. Signal Process., vol. 62, no. 9, pp. 2185–2199, May 2014.
9. Y. Zou, X. Wang, and W. Shen, “Optimal relay selection for physicallayer security in cooperative wireless networks,” IEEE J. Sel. Areas Commun., vol. 31, no. 10, pp. 2099–2111, Oct. 2013.
10. D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, “Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks,” IEEE J. Sel. Areas Commun., vol. 29, no. 10, pp. 2067–2076, Dec. 2011.