ISSN: 2348-2079

Volume-11 Issue-1

International Journal of Intellectual Advancements and Research in Engineering Computations

A Secure and Privacy Location Identify and Verification Process using Hybrid Hashing Techniques

K. Keerthana, Dr. B.S.Deepapriya

Scholar, Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Perunthurai, Erode – 638057, Tamilnadu, India
Assistant Professor, Department of Computer Science and Engineering, Erode Sengunthar Engineering College, Perunthurai , Erode – 638057, Tamilnadu, India.

Corresponding Author: Dr. B.S.Deepapriya
Published on: 26.03.2023

ABSTRACT

In Wireless Sensor Networks (WSNs), the discovery of neighboring nodes is a fundamental requirement for efficient communication and coordination. However, malicious nodes can forge their identities, leading to potential attacks on the network. This study proposes a novel approach for neighbor node verification in WSNs using a hashing table. The proposed method uses a hash function to assign a unique identifier to each node in the network. Nodes then broadcast their unique identifier, which is received by their neighboring nodes. Each node maintains a hash table of its neighboring nodes, and upon receiving a broadcast from a new node, the hash value is compared against the hash values in the table to verify the identity of the sender. Simulation results show that the proposed method is effective in detecting and rejecting malicious nodes and has low communication overhead compared to existing methods. The proposed approach is scalable and can be easily integrated into existing WSN protocols. The study demonstrates the potential of hashing table-based verification mechanisms for enhancing the security and reliability of WSNs.

Keywords: Traffic matrix, Routing table, hidden traffic.

INTRODUCTION

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering message must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are

significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network. An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. MANETs are self- organizing and self re-configureing multi hop wireless networks where, the structure of the networkchanges dynamically. This is mainly due to the mobility of the nodes. Nodes in these networks utilizethe same random access wireless channel, cooperating in a friendly manner to engaging themselves in multi hop forwarding. The nodes in thenetwork not only act as hosts but also as routers that route data to/from other nodes in network. MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies.

Mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperateby not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power, andlimited availability of resources such as battery power, bandwidth and memory. Therefore nodes have to cooperate for the integrity of the operation of the network. Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. In ad hocnetworks devices (also called nodes) act both as computers and routers. Most routing protocols lead nodes to exchange network topology information in order to establish communication routes. This information is sensitive and may become a target for malicious adversaries who intend to attack thenetwork or the applications running on it.

There are two sources of threats to routing protocols. The first comes from external attackers. Byinjecting erroneous routing information, replaying old routing information, or distorting routing information, an attacker could successfully partition a network or introduce a traffic overload by causing retransmission and inefficient routing. The second and more severe kind of threat comes from compromised nodes, which might (i) misuse routing information to other nodes or (ii) act on applicative data in order to induce service failures.

The provision of systematic approaches to evaluate the impact of such threats on particular routing protocols remains an open challenge today. Attacks on ad hoc are classified into non disruptive passive attacks and disruptive active attacks. The active attacks are further classified into internal attacks and external attacks are carried out by nodes that do not belong to network and can be preventedby firewalls and encryption techniques. Internalattacks are from internal nodes which are actually authorized nodes and part of the network hence it is difficult to identify.

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile usersthat communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobilenodes.

The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and deliveringmessages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea isnot easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routingpaths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recoveryfrom failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection orinterception. A lapse in any of these requirements may degrade the performance and dependability of the network.

Proposed scheme

Our proposed method involves two majorsteps to achieve our goals. Build point to point traffic matrices using the time slicing technique; derive end to end traffic matrices with a set of traffic filtering rules and a heuristic approach to identify actual source and destination nodes. Here all the MAC frames are encrypted so that the adversaries cannot decrypt them to look into the contents. For this padding technique is employed to all MAC frames have same size. Here MAC is set to broadcasting the address.

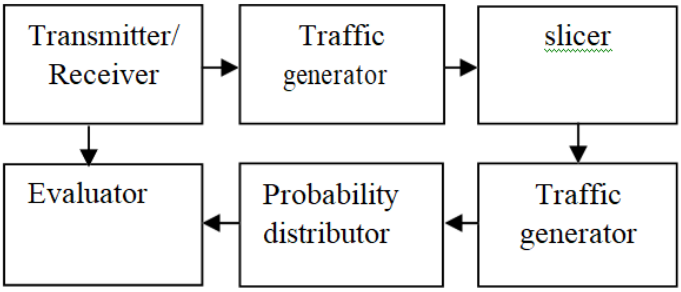
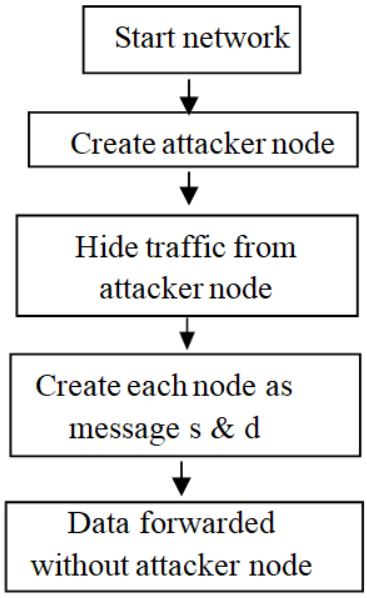


Fig 1: System model



s-source, d-destination

Fig 2: Data Flow Diagram

Topology Formation

Initially we are placing nodes in the network and wechoose a source and destination. If the source has no route to the destination, then source A initiates the route discovery in an on-demand fashion. After generating RREQ, node looks up its own neighbor. From this diagram, initially all the nodes form a network. Source node will establish a new route and it will start to send the data corresponding destination. We create a disclosure attack node; this node will try monitoring all the possible network routes. This one called us traffic monitoring. By creating message source and message destination probability distribution, and end-to-end to probability distribution. From these techniques we can easily hide the traffic from disclosure attack. Continue dataforwarding without hacker. It also includes,

Data Unit: Storing the data, accessing the data all aredone by this block.

Route Discovery: To find the new route includeRoute Request, Route Reply..

Route Maintenance: To check the availability of route in certain time intervals.

Timer: Calculate a time

Routing Table: This table contains all the necessary things about network such as source address, destination address, number of hops, next hop etc.

Routing Manager: To manage or control all the blocks.

This system provides more advantages as 1)Hidden traffic pattern can be discovered in good accuracy using STARS. 2)Identify all source and destination and find their relationship. 3)No information about the traffic patterns is disclosed from the routing layer and above. 4)Dummy trafficand delay are restricted.

System analysis

Modules

1. Topology Formation
2. Attacker Model
3. STAR
4. Traffic Protector

Table to find if it has any closer neighbor node toward the destination node. If a closer neighbor node is available, the RREQ packet is forwarded to that node. If no closer neighbor node is the RREQ packet is flooded to all neighbor nodes.

Fig 3: Route Discovery

When destinations receive the RREQ, it willgenerate RREP and it will send the same path. Finally we establish the route for data traffic.

Attacker Model

Here STARS including the attacker node which one monitors all the possible traffic patterns in the whole network. This attack is known as disclosure attack. Attackers only need to collect information and perform analysis quietly without changing the network behavior (such as injecting or modifying packets).

Star

STAR is the technique will create source/destination probability distribution for each and every node to be a message source and destination and the end-to-end link probability distribution(the probability for each node to be an end-to-end communication pair).

Traffic Pattern Discovery

Source/Destination Probability Distribution

The ability of STARS to identify the source and destination by calculating the source/destination probability distribution. The source probability distribution of (S1) and the destination probability distribution of (S2), are derived and the node with highest probability to be the destination, which match the simulation setup.

Traffic Protector

In this module, first it uses the captured traffic to construct a sequence of point-to-point trafficmatrices and then derives the end-to-end traffic matrix. Second, further analyzing the end-to-end traffic matrix, it calculates the probability for each node to be a source/destination (the source/destination probability distribution) and that for each pair of node to be an end-to-end communication link (the end-to-end link probability distribution). Finally it will hide the traffic pattern between actual source and destination from disclosure nodes.

Traffic Matrices Construction

Point-to-Point Traffic Matrix

With the captured point-to-point (one-hop) traffic in a certain period T , we first need to build point-to-point traffic matrices such that each traffic matrix only contains independent packets. Thus packets captured at different time could be the same packet appearing at different locations, such as the two packets sent by node 1 and node 2 consecutively, so they are "dependent" on each other. To avoid a single point-to-point traffic matrix from containing two dependent packets, we apply a "time slicing" technique. Let the traffic matrix be W_e, which is an N

N one-hop traffic relation matrix. The length of each time interval is determined by two criteria: 1) A node can be either a sender or a receiver within this time interval. But it cannot be both. 2) Each traffic matrix must correctly represent the one-hop transmission during the corresponding time interval.

End-to-End Traffic Matrix

Given a sequence of point-to-point traffic matricesour goal is to derive the end-to-end traffic matrix. Algorithm 1.

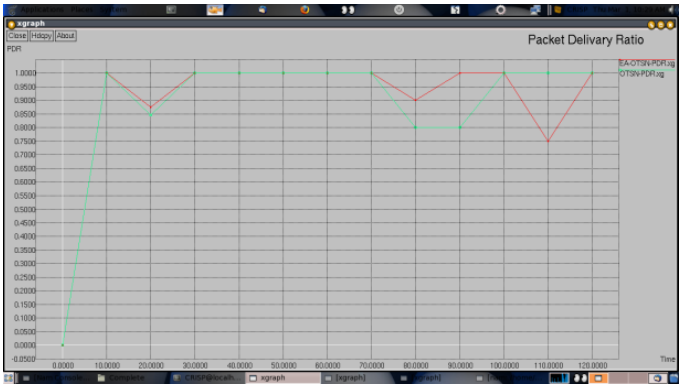
Experimental results

Simulating is a process of designing a modelof a real system and conducting experiments with this model for the purpose of understanding the behavior of the system and/or evaluating various strategies for the operation of the system. Simulation is widely-usedin system modeling for applications ranging from engineering research, business analysis, manufacturing planning, and biological science experimentation, just to name a few. Compared to analytical modeling, simulation usually requires less abstraction in the model (i.e., fewer simplifying assumptions) since almost every possible detail of the specifications of the system can be put into the simulation model to best describe the actual system. When the system is rather large and complex, a straightforward mathematical formulation may not be feasible. In this case, the simulation approach is usually preferred to the analytical approach.

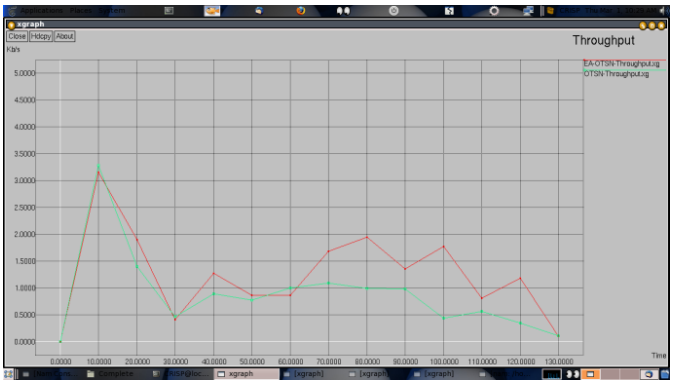
In common with analytical modeling, simulation modeling may leave out some details, since too many details may result in an unmanageable simulation and substantial computation effort. It is important to carefullyconsider a measure under consideration and not to include irrelevant detail into the simulation.

Traffic matrices to derive the end-to- end traffic matrix, traffic pattern by finding theprobability for each source and destination nodes and then correlate with its corresponding source and destination and then uses a heuristic data processing model to reveal the hidden traffic patterns from the end-to-end matrix. This can also be done using GStars. Our empirical study demonstrates that theexisting MANET systems can achieve very

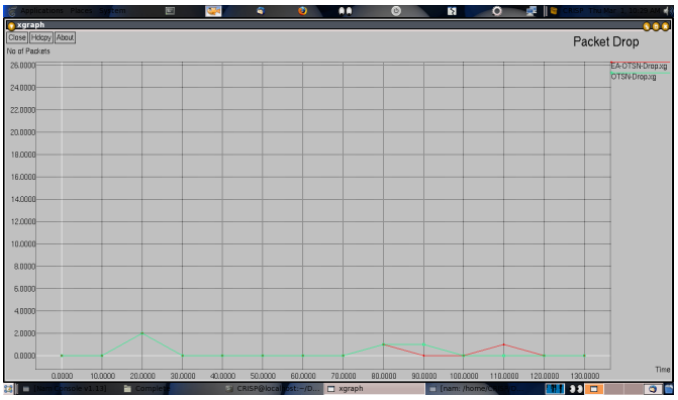
restricted communication anonymity with the use of AODV protocol under the attack of STARS, which produces good accuracy.



(IV.a) Performance Evaluation for Packet Deliver Ratio



IV.(b)Performance Evaluation for Time Delay



IV.(b)Performance Evaluation for Throghput

REFERENCES

1. Dai W. Available from: http://weidai.com/freedom-attacks.txt. Two Attacks against a PipeNet-like protocol once used by the freedom service; 2013.
2. Freudiger J, Manshaei MH, Hubaux J-P, Parkes DC. On non-cooperative location privacy: a game- theoretic analysis. In: Proceedings of the of ACM conference on computer and communications security; 2009. p. 324-37. doi: 10.1145/1653662.1653702.
3. Zhang C, Lu R, Lin X, Ho PH, Shen X. 'An efficient Identity based batch verification scheme for vehicular sensor networks,' in Proc. of the 27th IEEE International Conference on ComputerCommunications (Infocom), pp. 24650. Phoenix. Arizona; 2008.

4. Zhang C, Lin X, Lu R, Ho P-H. RAISE: an Efficient RSU aided Message Authentication Scheme in Vehicular Communication Networks. In: Proceedings of the of IEEE international conference on communications(ICC), Beijing, China; May 2008:1451-7. doi: 10.1109/ICC.2008.281.
5. Qin Y, Huang D. OLAR: on-demand lightweight anonymous routing in MANETs. In: Proceedings of the fourth int conf. mobile computing and ubiquitous networking (ICMU ’08); 2008. p. 72-9.
6. Shokri R, Yabandeh M, Yazdani N. Anonymous routing in MANET using random identifiers. In: Proceedings of the sixth int conf. networking (ICN ’07); 2007. p. 2. doi: 10.1109/ICN.2007.23.
7. Kong J, Hong X, Gerla M. An identity-free and on-demand routing scheme against anonymity threats in mobile ad hoc networks. IEEE Trans Mob Comput. August 2007;6(8):888-902. doi: 10.1109/TMC.2007.1021.
8. Wang X, Chen S, Jajodia S. Network flow watermarking attack on low-latency anonymous communication systems. In: Proceedings of the IEEE symposiumsecurity and privacy; 2007. p. 116-30. doi: 10.1109/SP.2007.30.
10. Seys S, Preneel B. ARM: anonymous routing protocol for mobile ad hoc networks. In: Proceedings of the IEEE 20th int conf. advanced information networking and applications workshops (AINA Workshops ’06); 2006. p. 133-7. doi: 10.1109/AINA.2006.104.