International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 2 Issue: 8 2312 – 2316

LD: Identifying Misbehaving Nodes in MANET

Tejaswi Bommi
Computer science Engineering
UCEK-JNTUK
Kakinada, India
Email: tejaswi.bommi9@gmail.com

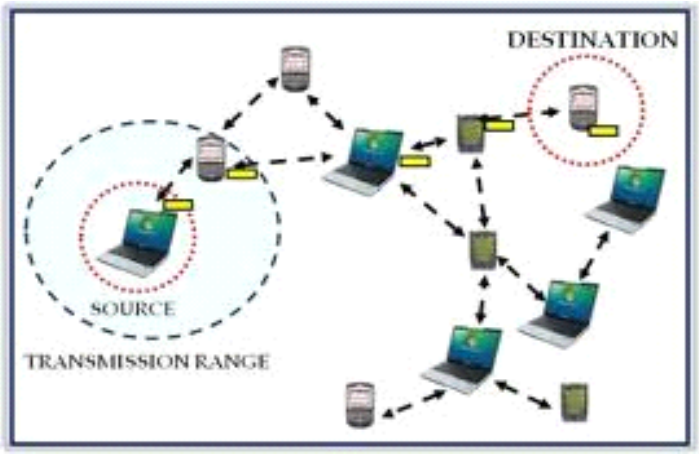
SSSN. Usha Devi N
Asst.prof, Computer science Engineering
UCEK-JNTUK
Kakinada, India
Email: usha.jntuk@gmail.com

***Abstract*--** A mobile ad-hoc network is a collection of mobile nodes connected together over a wireless medium without any fixed infrastructure. Unique characteristics of mobile ad-hoc networks such as open peer-to-peer network architecture, shared wireless medium and highly dynamic topology, pose various challenges to the security design. Mobile ad-hoc networks lack central administration or control, making them very vulnerable to attacks or disruption by faulty nodes in the absence of any security mechanisms. Also, the wireless channel in a mobile ad-hoc network is accessible to both legitimate network users and malicious attackers. So, the task of finding good solutions for these challenges plays a critical role in achieving the eventual success of mobile ad-hoc networks. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. Secure routing protocols and mechanisms to detect routing misbehavior in the direct neighborhood exist; however, collusion of misbehaving nodes has not been adequately addressed yet. We present LeakDetector, a mechanism to detect colluding malicious nodes in wireless multihop networks A mobile ad-hoc network is a collection of mobile nodes connected together over a wireless medium without any fixed infrastructure. Unique characteristics of mobile ad-hoc networks such as open peer-to-peer network architecture, shared wireless medium and highly dynamic topology, pose various challenges to the security design. Mobile ad-hoc networks lack central administration or control, making them very vulnerable to attacks or disruption by faulty nodes in the absence of any security mechanisms. Also, the wireless channel in a mobile ad-hoc network is accessible to both legitimate network users and malicious attackers. So, the task of finding good solutions for these challenges plays a critical role in achieving the eventual success of mobile ad-hoc networks. However,the. LeakDetector enables the calculation of the packet-loss ratio for the individual nodes.

*****

I. INTRODUCTION

The term MANET (Mobile Ad hoc Network) refers to a multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. Otherwise, a stand for "Mobile Ad Hoc Network" A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission.



Structure of MANET

The purpose of the MANET working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion and other factors. Approaches are intended to be relatively lightweight in nature, suitable for multiple hardware and wireless environments, and address scenarios where MANETs are deployed at the edges of an IP infrastructure. Hybrid mesh infrastructures (e.g., a mixture of fixed and mobile routers) should also be supported by MANET specifications and management features.

Using mature components from previous work on experimental reactive and proactive protocols, the WG will develop two Standards track routing protocol specifications

- Reactive MANET Protocol(RMP)
- ProactiveMANETProtocol(PMP)

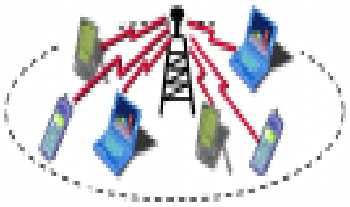
If significant commonality between RMRP and PMRP protocol modules is observed, the WG may decide to go with a converged approach. Both IPv4 and IPv6 will be supported. Routing security requirements and issues will also be addressed. The MANET WG will also develop a scoped forwarding protocol that can efficiently flood data packets to all participating MANET nodes. The primary purpose of this mechanism is a simplified best multicast forwarding function. The use of this protocol is intended to be applied ONLY within MANET routing areas and the WG effort will be limited to routing layer design issues. The MANET WG will pay attention to the OSPF-MANET protocol work within the OSPF WG and IRTF work that is addressing research topics related to MANET environments.

Characteristics of MANET's:

- In MANET, each node acts as both host and router. That is it is autonomous in behavior.
- Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.
- Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.
- The nodes can join or leave the network anytime, making the network topology dynamic in nature.
- Mobile nodes are characterized with less memory, power and light weight features.
- The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.
- Mobile and spontaneous behavior which demands minimum human intervention to configure the network.
- All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.
- High user density and large level of user mobility.
- Nodal connectivity is intermittent.

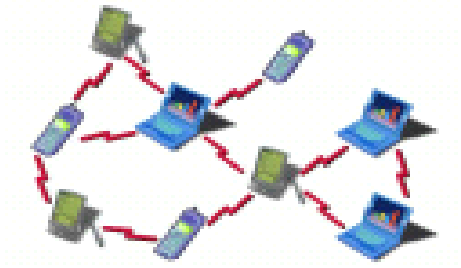
Infrastructure-based Networks:

- Fixed backbone
- Nodes communicate with access point
- Suitable for areas where APs are provided



Infrastructure-less Networks

- Without any backbone and access point
- Every station is simultaneously router



Nodes:

- limited resources
- dynamic topology
- Address assignment

Wireless channels:

- relatively high error rate
- high variability in the quality
- low bandwidth
- broadcast nature
- security aspect

Types of MANET:

There are different types of MANETs including:

- In VANETs – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.
- Vehicular ad hoc networks (VANETs) – Enables effective communication with another vehicle or helps to communicate with roadside equipments.
- Internet Based Mobile Ad hoc Networks (iMANET) – helps to link fixed as well as mobile nodes.

Types of routing protocols in the MANET:

Two types of routing protocols:

- Table-Driven Routing Protocols
  - Destination-Sequenced Distance-Vector Routing (DSDV)
  - Cluster head Gateway Switch Routing (CGSR)
  - The Wireless Routing Protocol (WRP)
- Source-Initiated On-Demand Routing Protocols
  - Ad-Hoc On-Demand Distance Vector Routing (AODV)
  - Dynamic Source Routing (DSR)
  - Temporally-Ordered Routing Algorithm (TORA)
  - Associativity-Based Routing (ABR)
  - Signal Stability Routing (SSR)

Advantages of MANET's:

- Wireless communication
- Mobility
- Do not need infrastructure
- but can use it, if available
- small, light equipment

II. LITERATURE REVIEW

Wireless communication represents a major industrial stake in the coming years. It offers numerous usages and helps industry save operating costs as well as improving operational efficiency. In the recent years, WiFi (IEEE 802.11- WLANs) and Bluetooth technologies (IEEE 802.15-WPANs) have known tremendous development and have penetrated small office and home office as well as large enterprise office. These general-public wireless technologies may find their limited usage in industrial installations because of harsh environments, electromagnetic compatibility and interference issues, safety and information technology (IT) security constraints, and battery autonomy[1]. In a mobile wireless ad hoc network, computers (nodes) in the network cooperate to forward packets for each other, due to the limited wireless transmission range of each individual node. The network route from some sender node to a destination node may require a

number of intermediate nodes to forward packets to create a ‘‘multihop’’ path from this sender to this destination. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed. Secure ad hoc network routing protocols are difficult to design, due to the generally highly dynamic nature of an ad hoc network and due to the need to operate efficiently with limited resources, including network bandwidth and the CPU processing capacity, memory, and battery power (energy) of each individual node in the network. We present the design and evaluation of a new secure ad hoc network routing protocol using distance vector routing[2].

Ad hoc networks are an increasingly promising area of research with lots of practical applications. However, MANETs are extremely vulnerable to attacks due to their dynamically changing topology, absence of conventional security infrastructures and open medium of communication, which, unlike their wired counterparts, cannot be secure. In this paper, we present our intrusion detection system
ExWatchdog, which is based on one proposed solution Watchdog. ExWatchdog solves a fatal problem of Watchdog, i.e., a malicious node can partition the network by falsely reporting other nodes as misbehaving. We use Throughput and Overhead as metrics to evaluate the performance of ExWatchdog with some nodes being malicious nodes that falsely report other nodes as misbehaving. For each metric, we test Watchdog and our solution separately. The simulation results show that our solution decrease the overhead greatly, though it doe not increase the throughput obviously[3]. Nodes directly communicate with each other when they are both within their communication ranges. Otherwise, they rely on their neighbors to store and forward packets[4]. The change of communication medium from physical cable to over the air has brought a lot of challenges to the computer communication security research. Due to the unique characteristics like open medium, changing topology and lack of centralized monitoring, MANETs are especially vulnerable to malicious attackers. There are mainly two types of attack in MANETs, namely active attack and passive attack. For passive attacks, packets containing secret information might be eavesdropped, which violates confidentiality. Examples include eavesdropping, traffic analysis and monitoring. Active attack, including injecting packets to invalid destinations into the network, deleting packets, modifying the contents of packets and impersonating other nodes violate availability, integrity, authentication and non-repudiation. Examples include jamming, spoofing, modification, replaying and Denial of Service (DoS). An individual mobile node may attempt to benefit from other nodes, but refuses to share its own resources. Such nodes are called selfish or misbehaving nodes, and their behavior is termed selfishness or misbehavior. One of the major sources of energy consumption in mobile nodes of MANETs is wireless transmission[4].Today wireless Sensor Networks has entered and
proved its efficiency in almost every application. Yet there are some metrics to holdback the security of the same, due to the very own attractive features of flexibility and open nature. Jamming of the medium to deny the service of a legitimate user is one among the many vulnerabilities of a wireless Sensor Network. A novel approach of marking the neighborhood packets forms a chain of legitimate message will preserve the originality at the other end and any packets to be found without the link information will be eliminated at the perimeter. This approach intends to provide a secure environment which withstands detection and mitigation as the principle[5]. Due to some special characteristics of MANETs, prevention mechanisms alone are not adequate to manage the secure networks. In this case detection should be focused as another part before an attacker can damage the structure of the system. First this paper gives an overview of IDS architecture for enhancing security level of MANETs based on security attributes and various algorithms, namely RSA and DSA. Then a hybrid cryptography IDS to further reduce the network overhead caused by digital signature is indicated[6]. open structure and scarcely available battery-based energy, node misbehaviors may exist. One such routing misbehavior is that some selfish nodes will participate in the route discovery and maintenance processes but refuse to forward data packets. we propose the 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme[7].

III. PROPOSED APPROACH

MODULES:

ACK implementation
Secure Acknowledgment (S-ACK)
Misbehavior Report Authentication (MRA)
Digital Signature Validation

MODULES DESCRIPTION:

ACK implementation:

ACK is basically an end – to – end acknowledgment scheme .It is a part of EAACK scheme aiming to reduce the network overhead when no network misbehavior is detected.

The basic flow is if Node A sends an packet p1 to destination Node D, if all the intermediate node are cooperative and successfully receives the request in the Node D. It will send an ACK to the source (Node A) , if ACK from the destination get delayed then it S-ACK process will be initialized.

Secure Acknowledgment (S-ACK):

In the S-ACK principle is to let every three consecutive nodes work in a group to detect misbehaving nodes. For every three consecutive nodes in the route, the third node is required to send an S-ACK acknowledgment packet to the first node. The intention of introducing S-ACK mode is to detect misbehaving nodes in the presence of receiver collision or limited transmission power.

Misbehavior Report Authentication (MRA):

The MRA scheme is designed to resolve the weakness of watchdog with respect to the false misbehavior report. In this source node checks the alternate route to reach destination.

Using the generated path if the packet reaches the destination then it is concluded as the false report.

Digital Signature Validation:

In all the three parts of EAACK, namely, ACK, S-ACK, and MRA, are acknowledgment-based detection schemes. They all rely on acknowledgment packets to detect misbehaviors in the network. Thus, it is extremely important to ensure that all acknowledgment packets in EAACK are authentic and untainted. Otherwise, if the attackers are smart enough to forge acknowledgment packets, all of the three schemes will be vulnerable.

Mobile Ad hoc Networks (MANET) or Wireless Mesh Networks (WMN) promise several benefits in comparison to the traditional single-hop wireless networks such as cellular networks. In MANETs and WMNs the range/capacity of the network is extended by active cooperation of the participating nodes. Nodes in the network act as routers and forward messages on behalf of the other nodes. The premise of node cooperation induces various challenging security issues.

One of the main issues in the process of routing of messages in the aforementioned class of networks is that the cooperation of nodes cannot be assumed in general. It can be beneficial for nodes to misbehave during the process of routing/forwarding, e.g. to save resources such as energy. A common attack is to drop messages of other nodes. Several approaches to detect routing/forwarding misbehavior in a node's one-hop neighborhood have been proposed. However, considering only the one-hop neighborhood disregards an important security problem: the collusion of misbehaving nodes.

Colluding misbehaving nodes are able to cloak the actions of each other in order to prevent detection of misbehavior. In Section II, we describe the problem of colluding misbehaving nodes in detail. We survey existing solutions to detect routing misbehavior (with and without collusion of misbehaving nodes) and highlight the shortcomings of these solutions to detect collusion of attackers in Section III. In Section IV, we state the assumptions for our solution to the problem and introduce *LeakDetector*, a mechanism to detect colluding misbehaving nodes in the network. Our solution comes with a low overhead and at no additional computational cost, as it requires no further cryptography. Section V presents the evaluation of our mechanism. We show that the *LeakDetector* is a very precise mechanism to detect misbehaving nodes that maliciously drop messages.

Colluding misbehaving nodes are a severe threat to the correct routing functionality in MANETs and WMNs. Before presenting *LeakDetector*, our solution for detecting colluding misbehaving nodes without the use of cryptography, we discuss the assumptions we made while designing the solution.

IV. A. Assumptions

The detection of misbehaving nodes depends on the underlying routing algorithm. For our scheme, we assume the following characteristics for this routing algorithm.

1) *Distributed & Unicast*: Each node autonomously calculates the next hop node; for each individual packet a single next hop neighbor is chosen.
2) *Proactive*: The routing mechanism periodically refreshes the routing information.
3) *Secure Route Information*: Message integrity and authenticity for routing messages is guaranteed; routing messages contain the information for the entire routing path.
4) *Multipath Routing*: Various paths from source to destination exist; *LeakDetector* compares these paths in order to identify malicious nodes.
5) *Single-hop Monitoring*: A watchdog (or similar) mechanism is in use for detecting routing misbehavior in the one-hop neighborhood.

B. Leak Detection Mechanism: Protocol

The main idea of *LeakDetector* is that the destination node of a route builds up a virtual graph, which models the multipath from the source node to the destination node. Periodic traffic information (which can be piggybacked on the proactive routing messages) enables the destination node to calculate the ratio of incoming and outgoing traffic—corresponding to the multipath routing information—for each participating node. Using graph theory, traffic leaks are identified. In particular, the destination node compares per route the incoming ratio with the outgoing ratio for each node participating. When the deviation is too large, the node is assumed to be malicious. The description of the leak detection mechanism and the actions and behavior of the individual nodes is as follows:

1) Source Node: each source node maintains a traffic counter per route (source-destination combination) denoting the amount of traffic (in bytes), which has been sent to the destination node.

We assume that the periodic proactive routing messages provide two fields, which are relevant for this task: T_{total} is used to describe the total traffic for this route (2 bytes); for each visited node i, T_i denotes the fraction of traffic that passed the node (1 byte per node) in comparison to the total traffic sent by the source node.

2) Intermediate Node: on its way from the source node S to the destination node D, the routing messages are forwarded by the intermediate nodes N_i. Let's assume the packet is forwarded from node N_1 to node N_2. Then N_2 performs the following steps: N_2 appends its own information to the visited node list, where the T_{total} field is already set. N_2 calculates the amount of traffic received from its precursor N_1 for the route $S \rightarrow D$. This amount of traffic is set in relation to the total traffic for this route (denoted in the T_{total} field of the routing message). The relation represents the fraction of traffic for this route sent from N_1 to N_2. N_2 sets the respective value in the T_{N1} field of the visited node entry. With the given parameterization of one byte for the T_{N1} field, we obtain a resolution of $100/255 = 0.4$ for the obtained fraction.

3) Destination Node: the destination node collects the traffic information from incoming routing messages and creates a virtual graph. Each vertex represents a node participating in a route from S to D. The directed edges between two nodes N_1 and N_2 represent the fraction of traffic that travels via $N_1 \rightarrow N_2$ on its path from S to D. The destination

 ISSN: 2321-8169
2312 – 2316

can also infer the amount of traffic sent from N_1 to N_2 corresponding to this route.

If D recognizes that the number of bytes received differs significantly from the number of bytes originated by the source, the *LeakDetector* enables the detection of the malicious node. The graph is further maintained and the amount of incoming traffic and outgoing traffic is updated with every incoming routing message for the corresponding nodes. If the values of a specific node X_1 differ significantly due to the outgoing traffic being far less than the incoming data, the destination node D assumes that X_1 is malicious.

4) Detection Criteria: a node in the route is not considered malicious if:

- the node is source S or destination D of the route.
- less than 50 packets have been received for this route (a minimal set of observations is required).
- the *inflow* of the node is smaller than 5% of total traffic or the difference of the *inflow* and the *outflow* of the node is smaller than 5% of total traffic.

If a node does *not* fit in the latter two categories, the node is considered malicious if:

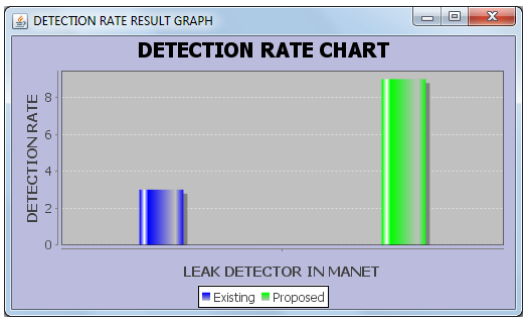
- $in_{node} > \alpha \cdot out_{node}$, with α being a tuning parameter for the *LeakDetector*.

If none of the aforementioned cases is applicable, a node is also considered benign.

5) Maintenance of Counter and Reconciliation of False Detections: Periodic initialization of the traffic counter (e.g., every 10 minutes) is necessary to allow the detection of nodes that switch to malicious behavior, but have previously cooperated. With a long-term history only, the system would only slowly react to such nodes. Resetting the counter should be loosely synchronized; in a time window of 30 seconds each node resets its internal traffic counter for the current route to 0. The destination node D of the route rebuilds the virtual graph.

Reaction to Malicious Nodes: once the destination node detects a node en-route as malicious, various strategies can be applied. E.g., the destination node may propagate this information to the source node, using a proactive route reply that uses a disjoint path. The source node could maintain a blacklist of nodes to avoid for routing/forwarding purposes. Also, the destination node can affect the route establishment and maintenance directly by marking or dropping routing messages that list malicious nodes in their path history. Another strategy would be to maintain reputation information in a distributed manner and to use this information to decide which paths to choose for a route and/or which nodes to punish

V. PERFORMANCE GRAPH



VI. CONCLUSION

Colluding malicious nodes are a severe risk for MANETs and WMNs, which rely on node collaboration. By working together, malicious nodes are able to trick well-behaving nodes. Their misbehavior is revealed only to other malicious nodes. We developed the mechanism to detect colluding malicious nodes. It can be used in combination with any proactive, multipath, non-broadcasting, secure routing algorithm. The *LeakDetector* is one of the first mechanisms for addressing the problem of malicious colluding nodes in WMNs.

Future work

Future research is to improve efficiency in leak detector methodology and decrease network overhead in MANET Caused by digital signature.

REFERENCES

[1] K. Al Agha , M.-H. Bertin, T. Dang, A. Guitton, P. Minet, T. Val, and J.-B. Viollet, "Which wireless technology for industrial wireless sensor networks? The development of OCARI technol, " *IEEE Trans. Ind. Elec- tron.*, vol. 56, no. 10, pp. 4266–4278, Oct. 2009

[2] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks, " in *Proc. 4th IEEE Workshop Mobile Comput. Syst. Appl.*, 2002, pp. 3–13.

[3] Nasser, N.Univ of Guelph**, Yunnfeng Chen "**Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks.communications, 2007.

[4] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowl- edgements in MANETs, " in *Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, Mar. 22–25, 2011, pp. 488–494.

[5] R. Akbani, T. Korkmaz, and G. V. S. Raju, "Mobile Ad hoc Net-work Security, " in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[6] R. H. Akbani, S. Patel, and D. C. Jinwala, "DoS attacks in mobile ad hoc networks: A survey, " in *Proc. 2nd Int. Meeting ACCT*, Rohtak, Haryana, India, 2012, pp. 535–541.

[7] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbe-haviour in MANETs, " *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, May 2007