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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Security, Trust and Resource Management in Mobile Ad- Hoc Wireless Networks

D. Madhu Babu, E. Bhargava Ram, B. Lakshmi Priya

Assistant Professor, Dept. of MCA, Narayana Engineering College, Nellore, AP, India

Student, Dept. of MCA, Narayana Engineering College, Nellore, AP, India

Student, Dept. of MCA, Narayana Engineering College, Nellore, AP, India

ABSTRACT: Mobility and security environment of Mobile Ad hoc Networks (MANET) is developed its popularity by two domains. MANETs have become a commonly used network for different applications. Linkage error and small packet progress, two sources for packet losses in mobile ad hoc network. A sequence of packet losses is present in the network. A distributed packet dropping attack (PDA) detection model is named as NAODV. Detection and isolation of small node is based on cooperative participation of nodes different communication based on TRUST level of the nodes. Conventional algorithms are based on noticing packet loss rate is satisfactory detection efficient the packet dropping rate is comparable to the channel error rate. The implement to detection efficient to correlations between lost packets is discovered. The packets are transmitted in the nodes with high trust value. SAODV is detecting small nodes by identifying dropping of network and data packet. Packet falling is link error and presence of malicious nodes is detected by SAODV. It also provides importance to security services of data. It decreases the computation overhead, a packet-block based method is proposed.

KEYWORDS: Wireless Adhoc Network, Public Auditing, Selective Dropping, TRUST, CONFIDENCE, decision tree. Auditing, AES, homomorphism linear signature.

I .INTRODUCTION

In a multi-hop wireless network, nodes get together in relay routing traffic. Assistant somebody will exploit thiscooperative nature to launch attacks. For instance the somebody might 1st faux to be a cooperative node within the route discovery method. Once being enclosed in a very route, the somebody starts dropping packets. Within the most severe type, the malicious node merely stops forwarding each packet received from upstream nodes, fully disrupting the trail between the supply and therefore the destination. Eventually, such a severe Denial-of Service(DOS) attack will paralyze the network by splitting its topology. Even though determined packet dropping will effectively destroy the performance of the network, from the attacker's viewpoint such subordinate "always-on" attack has its disadvantages. First, the continual presence of Extra ordinarily high packet loss rate at the malicious nodes makes this sort of attack simple to be detected. Second, once being identified, these attack area unit simple to moderate. for instance, just in case the attack is observed however the malicious nodes aren't known, one will use the irregular multi-path routing algorithms -vent the black holes formed by the attack, probabilistically eliminating the attacker. Vulnerability is a weakness in security system. A particular system may be susceptible to unauthorized data manipulation because the system does not verify a user's identity before permitting data access. MANET is more susceptible than wired network. Security is an essential service for wireless network communication.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Figure 1. Structure of mobile computing.

on plane, in car, on ship, etc. Thus, the discipline creates an illusion that the preferred data and sufficient processing power are available on the spot, where as in actuality they may be placed far away. Wireless ad hoc networks are collections of wireless nodes, that connect directly over common wireless channel. The nodes are equipped with wireless transceiver. They don't need any extra infrastructure, such as base station or wired access point, etc. Therefore, each node doesn't only shows the role of an end system, but also acts as a router, that sends packets to chosen nodes. The ad hoc are expected to do assignments, which the infrastructure can't do. Ad hoc networks are mostly used by military, rescue mission team, taxi drive

.

II. RELATED WORKS

Based on how much weight detection algorithm gives to link errors comparative to malicious packet drops, the works had been completed to detect the malicious packet dropping can be broadly classified into two. First group focuses on the detection with high malicious dropping rates, where the link errors are ignored. Based on the nature of the detection algorithm, this can be further classified into four. The first sub-group is based on credit systems.In this node gets incentive for its cooperation in broad cast .When the node correctly transmits the packets to the next hop, it gets credit. Based on the credit value ,the node gets priority through the transmission of its own packets. Thus, when the attacker nonstop drops packets, its credit decreases and automatically gets expelled from the network. But when the attacker performs a selectivedropping, it gets sufficient credits and can continue as a part of the network. The second sub category is based on reputation systems. In this mechanism the neighbour nodes maintains the activity of allnodes. For a node that drops packets maliciously gets a bad reputation. The reputation is the determining factor while selecting a route for transmission. Thus malicious nodes get excepted from a route. In this mechanism also, if the attacker selectively drop packets and forward some packets, then it can have a better reputation. The second category of works focus on the situation where the number of maliciously dropped packets is significantly higher than that affected by link errors, but the impact of link

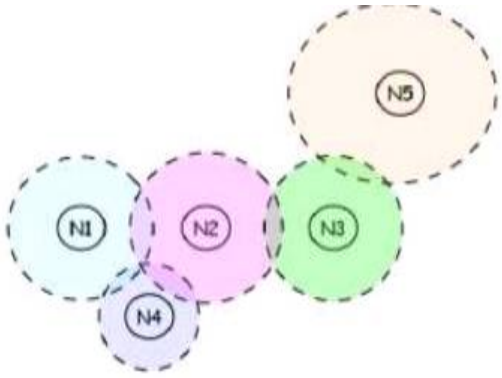


Figure 2. Transmission area in ad hoc

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

errors is no negligible. This type of mechanisms requires the knowledge of the wireless channel. The works in and proposed to detect malicious packet dropping by calculating the number of lost packets. If the number of lost packets is significantly higher than the expected packet loss rate made by link errors, then with high probability a malicious node is paying to packet losses. But counting the number of lost packets is not sufficient to identify the attacker. There are some unknown events, which cause access point's malfunction. The nodes lose their network and they are self-styled not working. It is the biggest infrastructure's disadvantage. There are
also some reasons to sacrifice or not to use access point's services. These can be cost factor, impossibility to install access point in short time, etc. In this case the nodes have to build its ownnetwork. This network is called wireless ad hoc network. The wireless ad hoc networks only consist of nodes equipped with transceiver. The network is created to be independent from an infrastructure. Therefore, the nodes must be able to arrange their own networks. A node can now communicate only with other nodes in its transmission range. In the infrastructure based wireless network, the nodes can communicate with a node, which is located in another network area, by transmitting data to destination access point and this access point relay the data to the desired node.

III. SECURED ADHOC ON DEMAND DISTANCEVECTOR ROUTING PROTOCOL

In SAODV is proposed by adding extra security featuresto AODV. Which offers privacy for preserving truthful detection of packet dropping attack in MANET Packet may be dropped through forwarding of routing information or through data forwarding. Dropping can be due to presents of malicious nodes or due to link errors. SAODV can investigate the dropping and can find the malicious node

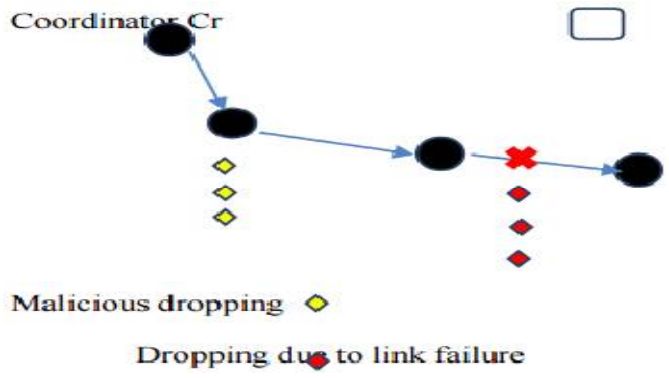


Figure 3. Network model

or failed link behind this dropping. For identifying data packet dropping attack cryptographic scheme is added in SAODV. In this approach after finding the source to destination path, all nodes involved in the path should forward its on public key to source node. Then the source node can encrypt the packet with public-key crypto-system such as RSA. Before the encryption process, the checksum value is counted for the whole message. Message is then separated into packets. Each packet and its checksum isencrypted with RSA algorithm. Encryption is starting by using the public key of the destination node and end by the public key of nearest neighbour node of source.

IV. PROPOSED METHODOLOGY

In the system model, low rates of packet loss or any additional packets drop other than malicious packet drop are assumed as threshold packet drop. When packet drop is higher than the threshold packet drop than PDA is suspected. PDA is suspected in certain node based on the different network performance parameters such as packet delivery ratio as well as output of the network. It is assumed that packets are forwarded in a hop by-hop

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

fashion in on demand ad hoc way. The communication links are expected to be bi-directional and there is no wireless channel error. All nodes use unidirectional antennas for bidirectional communications. Neighbour discovery protocol is assumed to be worked in such a way that every node can recognize its corresponding neighbor. It is assumed that all the nodes in MANET have the capability to recognize packet drop in them. Thus it has the ability to recognize the threshold packet drop as well as malicious packet drop

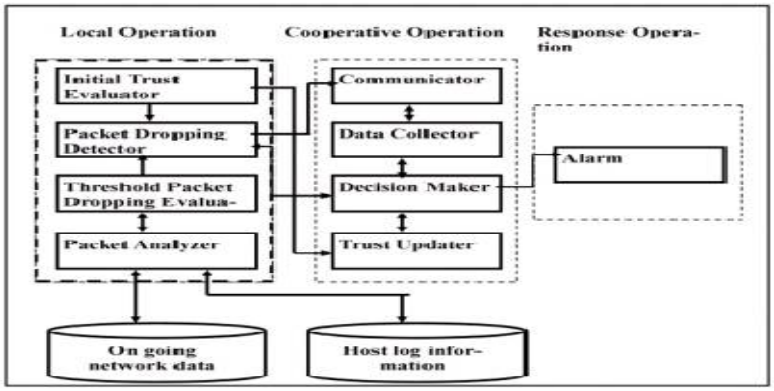


Figure 4. Schematic diagram of distributed PDA

detection methodology nodes in the communication. Activity of the agent is dependent on the network performance matrices such as: a. Delay in Delivery of the Packet
b. Response Time
c. Quality of Service Provider
d. Packet Forwarding Misbehavior
Proposed distributed PDA detection procedure is based on cooperation of different nodes. Data collected from different nodes are studied to detect PDA. Upon detection ,message will be distributed amongst the nodes in terms of alarm to escape the malicious nodes for packet forwarding. The total system is an automatic, self-controllable process. Data, collected from various nodes' host level audit system like "system log", are analyzed by the system. Then data abstraction is done on the collected data. As shown in Fig 1, different modules and their functions are discussed.

A. Proposed Detection Scheme
The proposed mechanism is based on detecting the correlations between the lost packets over each hop of the path. The basic idea is to model the packet loss process of a hop as a random process alternating between 0 (loss) and 1 (no loss). Specifically, consider that a sequence of M packets that are transmitted consecutively over a wireless channel. By observing whether the transmissionsare successful or not To develop an accurate algorithm for detecting selective packet drops made by insider attackers. This algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap–a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions.

B. Network and Channel Models
Consider associate absolute path PSD in a very multi hop wireless circumstantial network, as shown in Figure one. The supply node S easelessly sends packets to the destination node D through intermediate nodes n1, . ..,nK ,

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

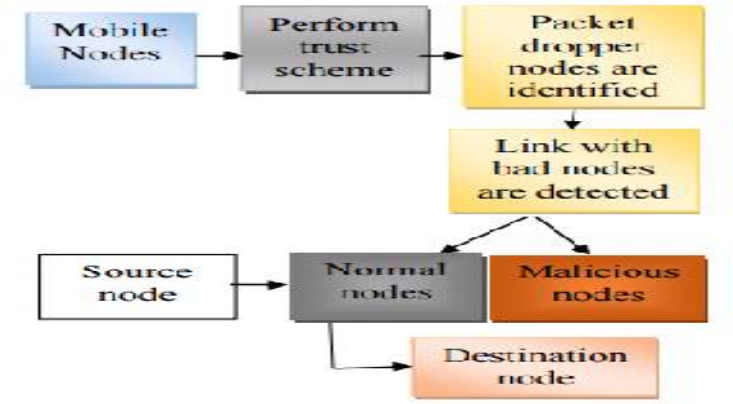


Figure 5. Block diagram of trust scheme

wherever Ni is that the upstream node of ni+1, for one i K one. we tend to assume that S is alert to the route PSD, as in Dynamic supply Routing (DSR) [15]. If DSR isn't used,S will establish the nodes in PSD by playing a trace route operation. Here we tend to in the main target visible once the quantity of maliciously born packets is comparable those caused by link errors. to properly calculate the correlation between lost packets, it's crucial to accumulate truthful packet-loss info at individual nodes. we tend to developed associate HLA-based public auditing design that ensures truthful packet-loss reportage by individual nodes. This design is collusion proof, needs comparatively high procedure capability at the supply node, however incurs low communication and storage overheads over the route. to scale back the computation overhead of the baseline construction, a packet-block-based mechanism was conjointly projected, that permits one to trade detection accuracy for lower computation complexness.

C. Audit Phase

This phase is triggered when the public auditor Ad receives an ADR message from S. The ADR message includes the id of the nodes on PSD, ordered in the downstream direction, i.e., n1, . . . , nK , S's HLA public key information pk = (v, g, u), the sequence numbers of the most recent M packets sent by S, and the sequencenumbers of the subset of these M packets that were received by D. Recall that we assume the information sent
by S and D is truthful, because detecting attacks is in their interest. Ad conducts the auditing process. Note that the above mechanism only guarantees that a node cannot understate its packet loss, i.e., it cannot claim the reception of a packet that it actually did not receive. This mechanism cannot prevent a node from overly stating its packet loss by claiming that it did not receive a packet that it actually received. This latter case is prevented by another mechanism discussed in the detection phase.

D. Detection Phase

The public auditor Ad enters the detection phase after receiving and auditing the reply to its challenge from all nodes on PSD. The main tasks of Ad in this phase include the following: detecting any overstatement of packet loss at each node, constructing a packet-loss bitmap for each hop, calculating the autocorrelation function for the packet loss on each hop, and deciding whether malicious behavior is present. More specifically, Ad performs the setasks as follows. The auditor calculates the autocorrelation function. The detection process applies to one end-to-end path. The detection for multiple paths can be performed as multiple independent detections, one for each path. Although the optimal error threshold that minimizes the detection error is still an open problem, our simulations show that through trial-and-error, one can easily find a good eth that provides a better detection accuracy than the optimal detection scheme that utilizes only the pad of the number of lost packets.

V. PERFORMANCE EVALUATION

For comparing performance of AODV and SAODV ONE simulator is used. It is a java based simulation tool. Main focus is truthful detection of packet dropping attack. Two separate MANET is created for this purpose and one is

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

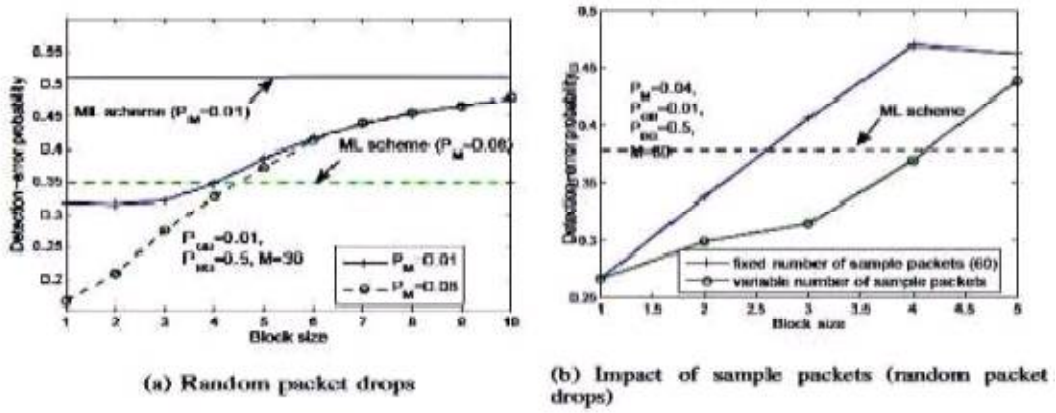
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

simulated with AODV and another with SAODV. From this experiment it is identified that routing complexityof SAODV is higher than AODV, but proper detectionof packet dropping attack can done by SAODV. As Compared to AODV, SAODV have very high detection rate. Experiment also shows that SAODV truthfully detect packet dropping attack in MANET. Simulation Setup The detection accuracy which can be achieved by the Conventional algorithm with the optimal maximum likelihood algorithm that utilizes the distribution of the number of lost packets. For given packet-loss bitmaps, the detection on different hops is conducted separately. So, only need to simulate the detection of one hop to evaluate the performance of a given algorithm. In all the simulated cases, the proposed algorithm can detect the actual cause of the packet drop more accurately than the ML scheme. Dropping of Control Packets The simulations so far have not made any application semantic (use case) assumption on the dropped packets. In reality, however, because these packets are usually used for control purposes, the loss of these packets may generate significant impacts on the transmission of other (i.e., data) packets.



(a) Random packet drops (b) Impact of sample packets (random packet drops)

Figure 6. Detection accuracy of block-based algorithms

Detection In this series of simulations, the detection accuracy of block-based algorithms as a function of block size In general, it shows that for both cases the detection error increases with the block size. This is expected, as a larger block size hides more details of packet losses, and therefore makes the actual correlation of lost packets more difficult to calculate. Meanwhile, the benefits of blocked-based algorithm is also observed. It is able to trade computation complexity for better detection accuracy

VI. CONCLUSION

An accurate method for detecting selective packet drops made by insider attackers is proposed in this paper. It also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. Mobile Ad hoc Network (MANET) is a type of Ad-hoc Network which changes its location dynamically and configures itself. MANET does not have a fixed topology which causes priorities to different kind of attacks. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap–a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions. The proposed methodology has been experimented in various networks settings with various parameters.

REFERENCES

[1] J. N. Arauz, "802.11 Markov channel modeling,"Ph.D.dissertation, School Inform. Sci., Univ. Pittsburgh, Pittsburgh, PA, USA, 2004

[2] B. Awerbuch, R. Curtmola, D.Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks,"ACM Trans. Inform.Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

[3] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle. Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs, In Proc. of the 33rd IEEE Conference on Local ComputerNetworks

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

(LCN), Dublin, Ireland, October 2007.
[4] Hayajneh.T, Krishnamurthy.P, Tipper.D, and Kim.T, "Detecting malicious packet dropping in the presence of collisions and channelerrors in wireless ad hoc networks"(2009).
[5] KozmaJr.W and Lazos.L "REAct: resource-efficient accountabilityfor node misbehavior in ad hoc networks based on random audits". Wireless Network Security,(2009)

BIOGRAPHY

Madhu Babu. D is a Assistant Professor in the Department of Master of Computer Applications, NarayanaEngineering College, Nellore. His research interest in Security,Trust And Resource Management in Mobile Ad- Hoc Wireless Networks

Bhargava Ram .E, completed master of computer applications in narayana engineering college, Nellore. His research interest isSecurity,Trust And Resource Management in Mobile Ad- Hoc Wireless Networks

Lakshmi priya .B, completed master of computer applications in narayana engineering college, Nellore. Her research interest isSecurity,Trust And Resource Management in Mobile Ad- Hoc Wireless Networks