Packet Proceed attacks in Mobile Ad hoc networks: Security and Reliable Detection

P. Swathi

Assistant Professor, MCA Department, AITS, RAJAMPET

Abstract

Mobile Ad hoc Networks (MANET) have grown in popularity due to its mobility and security features. MANETs are a popular network for a variety of purposes. Packet losses in mobile ad hoc networks can be caused by two things: linkage errors and tiny packets. The network is experiencing a series of packet losses. NAODV is a suggested detection model for distributed packet dropping attacks (PDAs). Small node detection and isolation are founded on team work involvement of nodes communicating in different ways dependent on their TRUST levels. The packet dropping rate is equivalent to the channel error rate, according to traditional techniques. Finding an effective method of detecting It's tough to make connections between lost packets. Packets are sent through nodes that have a high level of trust. We tested this with NS2 and found that it was faster. By recognizing network and data packet drops, SAODV detects tiny nodes. The existence of malicious nodes is detected by SAODV, which detects packet dropping as a link problem. It also places a premium on data security. It proposes a packet-block based technique that trades detection accuracy for lower computing complexity to decrease computation overhead. In comparison to standard approaches, the suggested model achieves a substantially higher detection efficiency.

keywords: MANET, SAODV, Denial-of-Service, AODV, MD5 algorithm.

1. INTRODUCTION

Nodes in a wireless network with several hops join cooperatively to impart huge cloud. At least one node will take advantage of this allied mentality to launch assaults. When someone is contained in a specific path, they begin losing packets. In the most extreme case, the rogue node simply stops forwarding each packet received from upstream nodes, thereby interrupting the supply chain and, as a result, the destination. By splitting the network's architecture, a strong Denial-of-Service (DoS) assault will eventually disable it. Despite the fact that prolonged packet dropping degrades network speed, such a "always-on" assault has drawbacks from the attacker's perspective. To begin with, the persistent existence of packet loss is very common at nodes that are malevolent, makes this type of assault is efficient to identify. Second, once discovered, these assaults are competently to counteract. For example, if the attack is identified but the malicious nodes are unknown, the multi-path routing that isn't straight methods [1][2] will be used to avoid the assault's black holes, hence probabilistically removing the attacker. A security system's vulnerability is a flaw in it. Because the system does not authenticate a user's identity before granting data access, it may be open to unwanted data modification. The vulnerability of MANET is greater than that of a wired network. In wireless network communications, security is a must-have service. The properties of MANETS, on the other hand, present both obstacles and possibilities in terms of accomplishing security requirements [3]. While travelling by aircraft, automobile, ship, or other mode of transportation, a user can access and change needed data. As a result, the discipline gives the impression that the needed data and processing capacity are immediately available, although they could, in fact, be situated elsewhere. Ad hoc wireless networks are made up of a group of wireless nodes sharing a single wireless channel. Wireless transceivers are installed on the nodes. No need to require any extra infrastructure like a base station or a wired access point, for example. As a result, each node not only operates as a router as well as an end system sending packets to the nodes that have been specified. The ad hoc team is supposed to do tasks that the infrastructure is unable to complete. Military, rescue operation teams, and taxi drivers all use ad hoc networks.

Fig 1: Structure of mobile computing

2. RELATED WORKS

The effort done to identify malicious packet drops may be roughly categorized into two categories depending on the weight given to link problems in contrast to malicious packet loss by a detection algorithm. The first group concentrates on malicious dropping rates with high detection rates, whereas link issues are disregarded. This may be divided into four categories based on the detecting algorithm's nature. Credit systems [4] are the first sub-category. This node receives a monetary reward for its transmission cooperation. Credit is given to the node when the packets are properly sent to the next hop. During the transmission of its own packets, the node is given precedence based on the credit value. As a result, if the attacker continues to lose packets, his or her credit will dwindle, and the attacker will be immediately kicked off the network. However, if the attacker uses selective dropping, it will receive enough credits to remain in the network. Renown management [5], [6], [7] [8] are the second subcategory. Neighbor nodes keep track of each other's activities through this technique. A node's reputation is tarnished when it drops packets deliberately. When it comes to choosing a transmission route, reputation is the deciding element. As a result, malicious nodes are blocked from participating in a route. If the attacker drops packets selectively while forwarding others, it can improve its reputation in this way as well. The second group of studies focuses on the case in which the quantity of maliciously lost packets is substantially larger than that produced by link faults, although link problems have a considerable impact. The wireless channel must be understood for this sort of mechanism to work. Counting the number of dropped packets was proposed in [9] and [10] as a way to identify dropped packets which are malicious. If the total count of dropped packets is much higher than the predicted rate of packet loss due to connection problems, a malicious node is almost certainly to blame. Counting the amount of dropped packets, on the other hand, isn't enough to find the attacker. The failure of an access point is caused by a number of unknown factors. Nodes suffer a loss contact they are using their network effectively unusable. It is by far the most serious flaw in infrastructure. There are other reasons to forego or refuse to use the services of an access point. Costs, inability to deploy access point in a timely manner, and so on are examples. The nodes must create their own network in this case. Wireless ad hoc networks are the name for this type of network. Only transceiver-equipped nodes make up wireless ad hoc networks. The network has been designed to be self-contained. As a result, each node must be able to set up its own network. Only other nodes in its transmission range can connect with a node now. As a result, each node must be able to set up its own network. Only other nodes in its transmission range can connect with a node now. The nodes in A wireless network that is based on infrastructure can connect with a node in a different network region by sending data to an end point of access, which then relays the data to the target node. The ad hoc networks appear to be insufficiently strong. Each node has its own transmission range, which may be merged to generate a much larger transmission region. Single or multiple hopping strategies are used by the nodes to send data. Now, in order to improve the efficiency of data transmission, an appropriate routing algorithm must be created.

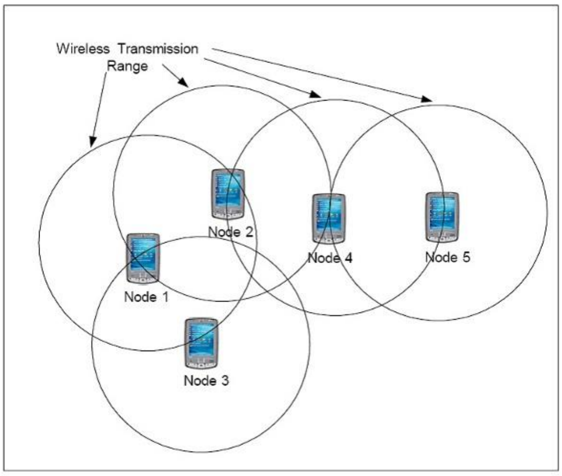
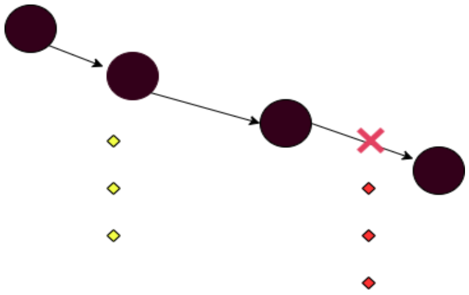


Fig 2: Transmission area in Adhoc

3. DISTANCEVECTOR ROUTING PROTOCOL SECURED AD HOC ON DEMAND

Adding more security elements to AODV is proposed in SAODV. Which method ensures privacy while maintaining the accuracy of packet dropping attack detection in a MANET? During routing information forwarding or data forwarding, packets may be lost. Dropping can occur as a result of the presence of malicious nodes or as a result of a link failure. SAODV can look into the drop and discover the malicious node or broken link that caused it. In SAODV, a cryptographic technique is implemented for detecting data packet dropping attacks. After determining the start-to-end path, all nodes along the path should provide their public key to the source node. The packet is then encrypted by the source node using a public-key cryptographic method like

RSA. The checksum value for the entire message is computed prior to the encryption procedure. Following that, the message is split into packets. The RSA method encrypts each packet as well as its checksum. The public key of the destination node is used to begin encryption, followed based on public key of the source's node with the closest neighbor. MD5 algorithm [11] is used to calculate the checksum.



Yellow color drop indicates Malicious dropping , Red drop indicates Dropping due to link failure

Fig.3. model of a network

4. PROPOSED METHODOLOGY

Packet loss is minimal or other packet drops, Apart from malicious packet drops, are presumed to be package with a certain size limit drops in the system model. PDA is suspected when packet loss exceeds the threshold. Based on network performance characteristics such as packet delivery ratio and network speed, PDA is suspected on a certain node. Packets are supposed to be transferred on demand using a hop-by-hop approach. There is no wireless channel error, and the communication channels are believed to be bi-directional. Bidirectional communication is carried out by all nodes using unidirectional antennas. The process for discovering your neighbors is supposed to be implemented in such a way that each node is aware of its neighbors. All MANET nodes are believed to be capable of understanding packet loss. As a result, it can distinguish between malicious and threshold packet drops. Source routing enables the promiscuous mode of the node. A rogue node has the ability to discard packets indefinitely or on a per-packet basis. More than one node's cooperation isn't taken into account here, thus malevolent nodes can observe and collaborate while masking their own wrongdoing. We believe that intelligent agents should be able to alter their decision-making by working with other communication nodes. The agent's actions are influenced by network performance matrices like:

Packet Delivery Delay a. Response Time b. Service Provider Quality c. Packet Forwarding Misconduct

The preferred decentralized PDA detection technology relies on several nodes cooperating. PDA is detected by analyzing data obtained from various nodes. When a malicious node is discovered, a message will be sent to all nodes in the form of an alert to prevent packet forwarding by malicious nodes. The entire procedure is fully automated and self-contained. The system analyses data obtained from host-level audit system for various nodes, such as "system log." Following that, the obtained data is abstracted. Various modules and their roles are addressed, as indicated in.

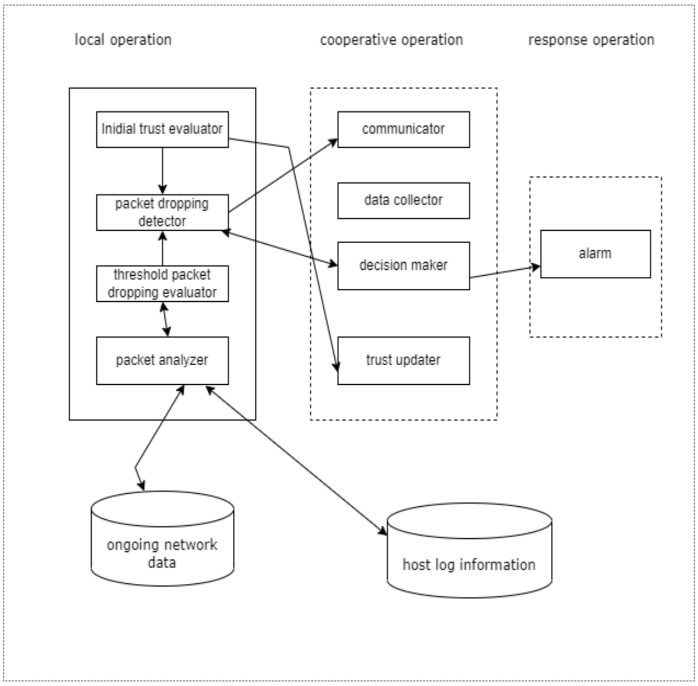


Fig.4: distributed PDA detection diagram

4.1 Preferred recognition Scheme

The suggested approach is according to the detection of anomalies. The relationships between the packets that were lost over time each step along the way The primary concept is to create a model. A hop's packet loss process like arbitrary process oscillating between 0 (loss) and 1 (hit). Consider the following example: a serial of M packets are sent in a row over a network

Channel for wireless communication. By looking at whether one can obtain an understanding of whether transmissions are successful or not technique for recognizing specific packets that is correct Insider attackers dump bombs. The method operates in this manner. As evidence to support the claim decision on detection, it also provides a credible and publicly verified source of information preference data.

4.2 Models of Networks and Channels

Consider a multichip wireless circumstantial network with associated absolute path PSD, as depicted in the following example. The supply node S continuously sends packets to the destination node D via intermediate nodes n_1,..., n_K, where Ni is the upstream node of ni+1, for one I K one. As in Dynamic Supply Routing (DSR) [12], we assume that S is aware of the route PSD. If DSR isn't utilized, S will execute a trace route operation to establish the nodes in PSD. When the number of fraudulently crafted packets equals the number of connection problem packets, we prefer to make the principal target visible. It's critical to collect accurate packet-loss data at individual nodes in order to determine the correlation between lost packets correctly.

We HLA-based public associations have a tendency to form auditing design that assures accurate packet-loss reporting Individual node reporting. This style is unique. Collusion-proofing, which necessitates a somewhat high level of expertise. Nonetheless, procedure capabilities at the supply node entails little transmission and cost of storage over the path to reduce the computation's size. To decrease the baseline construction overhead, a packet block-based method was also adopted. Allowing for the trade-off of detection precision for a decrease in computation complexity was envisioned.

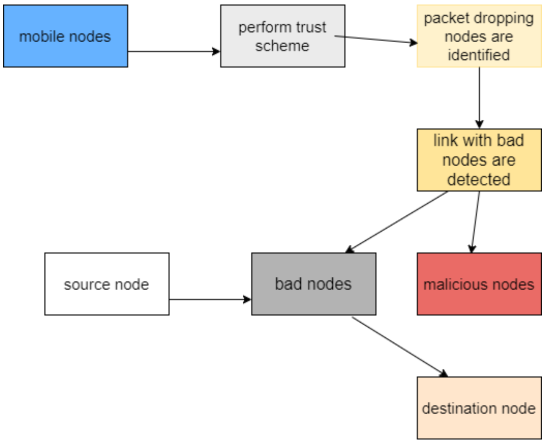


Fig. 5 Trust Scheme Block Diagram

4.3 Audit Phase

When Ad, the public auditor, gets an ADR communication from S, this step is activated. The ADR message contains the IDs of the nodes on PSD, ordered downstream, i.e., n1,..., nK, S's HLA public key information pk = (v, g, u), the sequence numbers of the most recent M packets transmitted by S, and the sequence numbers of the subset of these M packets received by D. Remember that we presume S and D are telling the truth since it is in their best interests for them to identify assaults. The auditing is carried out by Ad. Note that the foregoing approach merely ensures that a node cannot understate its packet loss, i.e., it cannot claim to have received a packet it did not. This method can't stop a node from exaggerating its packet loss by saying it didn't get a packet it did. Another mechanism, detailed in the detection step, prevents this later scenario.

4.4 Detection Phase

The public auditor is a person who is appointed by the government. The ad starts the detection phase after receiving and reviewing all node replies to the PSD challenge. The major objectives of Ad in this phase are to detect any overstatement of packet loss at each node, generate a packet-loss bitmap for each hop, compute the autocorrelation function for each hop's packet loss, and determine whether malicious activity is there. These are the duties that Ad carries out in more detail. Autocorrelation function is calculated by the auditor. The detection procedure is only applicable to a single end-to-end route. Multiple independent detections, one for each path, can be used to detect multiple paths. Although the ideal error threshold for reducing detection error is unknown and it is shown that by performing tests and finding defects, one can rapidly find a value that results in better detection accuracy than the optimal detection approach, which just counts the number of lost packets.

5. EVALUATION OF PERFORMANCE

SAODV correctly detects packet dropping attacks in MANET, according to the experiment.

5.1 Setup for Simulation

The detection accuracy that can be achieved by combining the popular technique, which depends on the distribution of lost packets and uses the optimum maximum likelihood algorithm. The detection of bitmaps of packet loss on various hops is done separately for each packet-loss bitmap provided. All that is required to evaluate the performance of a method is to mimic the detection of one hop.

5.2 Dropping Only Specific Packets

As a function of the count of intentionally irrecoverable packets, the rediscovery error increases. Similar performance patterns can be seen when random packets are dropped. When there are more packets maliciously dropped, both algorithms make fewer detection errors. The proposed technique outperforms the ML scheme in all simulated instances in detecting the true source of packet drops.

5.3 Control Packets are dropped

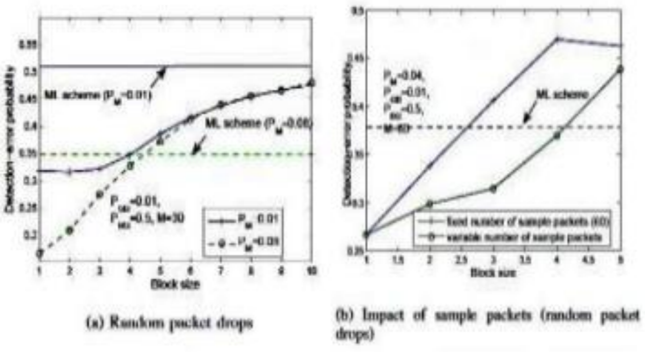
So far, no application semantic (use case) assumptions about missed packets have been made in the simulations. Packets are frequently employed for control, their loss could disrupt the transmission of other (data) packets. To see how the similitude between the data and control packets influences the performance of the introduced approach, we executed a series of simulations.

5.4 Detection based on blocks

The detection accuracy of block-based algorithms as a function of block size is investigated in this set of simulations. The diagnosed issue appears to develop with the block in all situations. This is to be anticipated, as a bigger size of block obscures more information about packet loss, making it more difficult to pinpoint the underlying cause of packet loss. At the same time, the advantages of a blocked-based method may be proven. It is feasible to establish a balance between processing complexity and accuracy in detection.

6. RESULT ANALYSIS

A single simulator was utilized to compare the performance of AODV and SAODV. It's a simulation tool that uses Java. The primary focus is on accurate packet dropping detection. For this aim, two distinct MANETs are formed, one using AODV and the other using SAODV. The routing complexity of SAODV is larger than AODV, according to this experiment, however SAODV can detect packet dropping attacks correctly. SAODV has a high detection rate when compared to AODV.



(a) Random packet drops

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

Fig 6. Detection accuracy of block-based algorithms

7. CONCLUSION

This study proposes a reliable approach for identifying selective packet drops done by attackers. It also gives accurate and publicly verifiable decision data as confirmation that the detection choice was made correctly. MANET is a sort of Ad-hoc Network that dynamically updates its position and manipulates itself. Because MANET has no set topology, different types of assaults are prioritized. To achieve high detection accuracy, the packet-loss bitmap's auto-correlation function (ACF)–a bitmap indicating the lost/received status of each packet in a sequence of sequential packet transmissions–is used to leverage correlations between the locations of lost packets. The suggested approach has been tested in a variety of network configurations with a variety of parameters. The outcomes are compared and studied against two other systems. The collaborative malicious packet dropping as well as battery power consumption are not taken into account in this technique. Furthermore, the "No answer" condition is not taken into consideration. In future investigations, the suggested mechanism's implementation and optimization under various protocols will be studied.

8. FURTHER WORKS

This work might be expanded in the future to identify malicious selfish nodes and malicious nodes behaving as selfish nodes. Unlike previous techniques, which rely solely on the distribution of lost packet numbers, the algorithm to make a better informed judgment, look at cross statistics between lost packets. When compared to previous detection methods that depend solely on the distribution of lost packet numbers, this method is far more effective. utilizing the correlation between dropped packets enhances the accuracy of identifying malicious packet drops dramatically.

REFERENCES

[1] Liu.K, Deng.J, Varshney.P, and Balakrishnan.K “An acknowledgement-based approach for the detection of routing misbehavior in MANETs”. Vol. 6, no.5, pp.536–550, May 2006

[2] Y. Liu and Y. R. Yang.name propagation and agreement in mobile ad-hoc networks. In Proceedings of the IEEE WCNC Conference, pages 1510–1515, 2003.

[3] K. Balakrishnan, J. Deng, and P. K. Varshney, “TWOACK: Preventing selfishness in mobile ad hoc networks,” in Proc. IEEEWirelessCommun. Netw. Conf., 2005, pp. 2137–2142.

[4] Malhotra. A, Kirtani.S ,Agarwal.T “Detection of malicious route in wireless adhoc networks” PP. 1-4, Mar 2010.

[5] 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 (LCN), Dublin, Ireland, October 2007.

[6] W. Yu, Y. Sun and K. R. Liu, HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks, In Proc. 24th IEEE INFOCOM, Miami, USA, March 2005.

[7] 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).

[8] KozmaJr.W and Lazos.L "REAct: resource-efficient accountabilityfor node misbehavior in ad hoc networks based on random audits". Wireless Network Security, (2009)

[9] Agarwal.T,Malhotra. A, Kirtani.S , "Detection of malicious route in wireless adhoc networks" PP. 1-4, Mar 2010.

[10] Ateniese.C, Burns.R, Curtmola.R, Herring.J, Kissner.L, Peterson.Z, and Song.D, "Provable data possession at untrusted stores"., pages 598–610, Oct. 2007.

[11] W. Kozma Jr. and L. Lazos.REAct: resource-efficient answerability for node misconduct in circumstantial networks supportedrandom audits. In Proceedings of the ACM Conference on Wireless Network Security (WiSec), 2009.

[12] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the ACM MobiHoc Conference, pages 46–57, 2005.

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

[14] 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.

[15] Julian Benadit.P, SharmilaBaskaran and RamyaTaimanessamy, "Detecting Malicious Packet Dropping Using Statistical Traffic Patterns", IJCSI International Journal of Computer Science Issues(2011), Vol.8, Issue 3, No. 2, ISSN (Online): 1694-0814

[16] V. MadhuViswanatham and A.A. Chari, "An Approach for Detecting Attacks in Mobile Adhoc Networks", Journal of Computer Science 2008, Volume 4, Issue 3, Pages 245-251 [17] Ricardo Puttini, Jean-Marc Percher, LudovicMé and Rafael de Sousa, "A Fully Distributed IDS for MANET", Computers and Communications, 2004. Proceedings.ISCC 2004. Vol. 1, Page(s): 331 – 338, Print ISBN: 0-7803-8623- X

[18] D. B. Johnson, D. A. Maltz, and J. Broch. DSR: the dynamic source routing protocol for multi-hop wireless ad hoc networks. Chapter 5, Ad Hoc Networking, Addison-Wesley, pages 139–172, 2001.

[19] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the ACM MobiHoc Conference, pages 46–57, 2005.

[20] A. Proano and L. Lazos. Selective jamming attacks in wireless networks. In Proceedings of the IEEE ICC Conference, pages 1–6, 2010.

[21] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan.associate acknowledgement-based approach for the detection of routing misbehav-ior in MANETs. IEEE Transactions on Mobile Computing, 6(5):536– 550, May 2006.

[22] G. Ateniese, S. Kamara, and J. Katz, ―Proofs of storage from homomorphic identification protocols,‖ in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security, 2009, pp. 319– 333.

[23] 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. Inf. Syst. Secur., vol. 10, no. 4, pp. 11–35, 2008.

AUTHORS PROFILE

P.Swathi is an Asssistant Professor in Master of Computer Applications Department at Annamacharya Institute of Technology and Sciences(Autonomous), Rajampet, Kadapa district. She received her Master's degrees in Computer Science(M.Tech) and MCA in 2015 and 2007, respectively, Jawaharlal Nehru Technological University . She is having 14 years of teaching experience. She is interested in Teaching Computer Networks ,Object Oriented Analysis and Design with UML ,Operating Systems, Data Mining , Network Programming, , Cryptography etc.