International Journal of Computer Sciences
July'2016 Issue
ISSN Number: 4142 3453

CONTROLLING DROPPING ATTACKS THROUGH THRUTHFUL DETECTION AS PACKETS IN WIRELESS ADHOC NETWORKS

N. Siva[1], P. Phanindra Kumar Reddy[2], Dr. A. Subramanyam[3]

[1]M.Tech.,(PG Scholar), Annamacharya Institute Of Technology & Sciences, Rajampet, Kadapa,
Email:nsiva546.rjpt@gmail.com
[2]Assistant Professor, Annamacharya Institute Of Technology & Sciences, Rajampet, Kadapa
Email: phanindra.44u@gmail.com
[3]Professor,HOD, Dept of CSE,Annamacharya Institute Of Technology & Sciences,Rajampet, Kadapa

ABSTRACT:

In a Wireless Ad Hoc Network, nodes collaborate in supporting the network functionality. The effect of malicious nodes can lead to Packet Dropping, which disrupt the communications of potentially any node within the ad hoc networking domain. Link errors cause packet dropping, so does the insider attack, or the combined effect of link errors and malicious nodes cause packet dropping. Multi-hop wireless ad-hoc network gives increased coverage and provide several benefits over traditional wireless local area networks. This architecture makes it more vulnerable to internal attacks from compromised nodes. One of them is packet dropping attack which is a crucial issue in networks. Link error and malicious packet dropping are two sources for packet losses. While observing a sequence of packet losses in the network, it is difficult to identify whether the loss is due to link errors or malicious nodes. This paper focuses on the insider-attack case, whereby malicious nodes that are part of the route selectively drop a small amount of packets which are critical to the network performance. Mobility and portable nature of Mobile Ad hoc Networks (MANET) has increased its popularity by two fold. MANETs have become a commonly used network for various applications. But this advantage suffers with serious security concerns, mainly a wireless transmission medium perspective where such networks may be subject to packet dropping. Mobility and portable nature of Mobile Ad hoc Network may also lead to link failure. During packet forward, valuable packets may be dropped by malicious nodes present in the network. Link error and malicious packet dropping are the two sources for packet losses in MANET. A node can act maliciously and could harm the packet sending process. In this paper, a public auditing system is used which allows the detector to verify the truthfulness of the packet loss information. The proposed mechanism is privacy preserving, collusion proof, and it incurs low communication and storage overheads at intermediate nodes. The proposed mechanism achieves better detection accuracy than the conventional methods such as a maximum-likelihood based detection.

Index Terms- Packet Dropping, Auditing, Attack Detection, Secure Routing

1. INTRODUCTION

In a multi-hop wireless network, nodes cooperate in relaying/routing traffic. An adversary can exploit this cooperative nature to launch attacks. For example, the adversary may first pretend to be a cooperative node in the route discovery process. Once being included in a route, the adversary starts dropping packets. In the most severe form, the malicious node simply stops forwarding every packet received from upstream nodes, completely disrupting the path between the source and the destination. Eventually, such a severe Denial-of-Service (DoS) attack can paralyze the network by partitioning its topology.

There are different reasons for packet loss which is shown in fig.1. A malicious node that is part of the route can exploit its knowledge of the network protocol and the communication context to launch an insider attack–an attack that is intermittent, but can achieve the same performance degradation effect as a persistent attack at a much lower risk of being detected. Specifically, the malicious node may evaluate the importance of various packets, and then drop the small amounts that are deemed highly critical to the operation of the network. For example, in a frequency-hopping network, these could be the packets that convey frequency hopping sequences for network-wide frequency-hopping synchronization; in

an ad hoc cognitive radio network, they could be the packets that carry the idle channel lists (i.e., white spaces) that are used to establish a network-wide control channel. By targeting these highly critical packets, intermittent insider attacker can cause significant damage to the network with low probability of being caught. In this paper, we are interested in combating such an insider attack. In particular, we are interested in the problem of detecting the occurrence of selective packet drops and identifying the malicious node(s) responsible for these drops.

In this paper, we develop an accurate algorithm for detecting selective packet drops made by insider attackers. Our algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision.

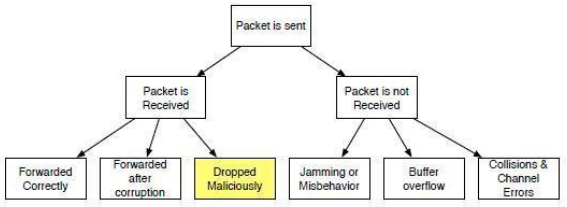

Fig 1: Overview of Packet Losses

The existing solutions for identifying misbehaving nodes use per-packet evaluation of peer behavior such as the 2ACK technique which detects the misbehaving links. Per-packet behavior evaluation is based on transmission overhearing or achieving of per-packet acknowledgement. This type of monitoring operations must be repeated on every hop, thus it requires high communication overhead and energy expenditure on a multi-hop network. The requirement of focusing the location (or hop) the packet is dropped and to identify whether the drop is intentional or not. The packet drop in the network could be caused by channel conditions such as fading, noise, interference or the link errors or by the insider attack. Link errors are significant in packet dropping considering the insider attack which can camouflage the technique of packet loss rate. Just observing the packet loss rate cannot accurately identify the cause of a packet loss. The high detection accuracy can be attained by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of packet-loss bitmap (describes the lost/received status of each packet in a sequence of consecutive packet transmissions). By detecting the correlation between the lost packets, one can decide whether the packet loss is purely due to link errors, or by the combined effect of malicious drop and link erro

II. RELATED WORK

In the year 2003, R. Rao and G. Kesidis proposed a paper titled "Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited" which observes the traffic patterns for the detection of packet dropping attacks. Sensors are used to check the traffic intensity. The network misinterpret the cause of packet loss as congestion instead of malicious activity. This paper suggests a traffic transmission patterns to be selected so that the verification can be made by a receiver. Such traffic patterns are used with suboptimal MAC that preserves the statistical regularity from hop to hop. This general technique for intrusion detection is therefore suitable for networks that are not bandwidth limited but have strict security requirements and thus the proposed system cannot be implemented in a bandwidth limited networks. In the year 2010, Tao Shu, Sisi Liu, and Marwan Krunz proposed a paper titled, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes" where a multipath scheme is explained. So once an adversary acquires the routing algorithm, it can compute the same routes known to the source, and hence endanger all information sent over these routes. The adversary cannot identify the routes traversed by each packet. Besides randomness, the routes generated by this mechanisms are also highly dispersive and energy-efficient, making them quite capable of bypassing black holes at low energy cost. This paper, develops a mechanism that generate randomized multipath routes. But extensive simulations are to be conducted and hence this is highly expensive method. Later on, in the year 2012, Alejandro Proan˜o and Loukas Lazos proposed a papertitled, "Packet-Hiding Methods for Preventing Selective Jamming Attacks" In this paper, the problem of jamming under an internal threat model. The adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack is considered. The adversary exploits the internal knowledge for launching selective jamming attacks in which it targets on "high importance" messages. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. The packet hiding Methods are based on several cryptographic primitives. Hence the computational and communication overhead is an issue. And in the year 2014 Kennedy Edemacu, Martin Euku and Richard Ssekibuule proposed "Packet drop attack detection techniques in wireless ad hoc networks: a review" which provides numerous techniques based on

reputation module, route discovery module, audit module referred as the AMD system. These modules closely interact to coordinate the functions of misbehavior detection, discovery of trustworthy routes, and evaluation of the reputation of peers. The schematic on the relationship between the three modules of AMD is as shown in the figure.

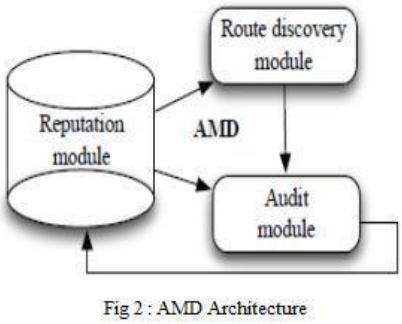

Fig 2 : AMD Architecture

Fig 2: AMD Architecture

The related work can be classified into the following two categories. The first category aims at the malicious packet dropping rates, which is based on the insider attacks. Here the impact of link errors is ignored. Credit systems, reputation systems, hop-to-hop acknowledgements and several cryptographic methods are used in this category.

A. The credit system provides an incentive for cooperation where the nodes receives credit by relaying packets for others. Thus the credits of malicious nodes are depleted due to the continuous drop of packets.

B. The reputation system is based on monitoring and identifying the misbehaving nodes. The neighbors are used for this purpose where the node with high packet dropping rate is given a bad reputation by its neighbors. This information is propagated throughout the network and is used as a metric in selecting routes.

C. An end-to-end or hop-to-hop acknowledgement directly locates the packet drop.

D. Cryptographic methods can also be used in identifying the malicious packet dropping rates.

The Second category is based on the number of maliciously dropped packets, but the drops caused by link errors are not negligible. Hence the source traffic rate with the estimated received rate is compared. This provides the information within a reasonable range and thus one can identify whether the drop is based on impairments or due to the malicious dropping.

Issues in conventional methods: These methods do not perform well when the packet dropping is highly selective.

1. In the credit based method, malicious nodes can gain the credit by forwarding packets it received.

2. In a reputation-based method, similar as in previous approach the reputation can be attained by forwarding the packets to the next hop. Thus a good reputation is maintained.

3. The acknowledgement-based method and the mechanisms in the second category, focuses on counting the number of lost packets. This is not sufficient to detect the malicious node causing the packet losses.

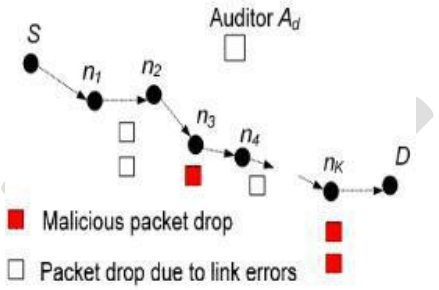

Fig 3: Network Model

Because the packet drop is highly selective, the detection accuracy of these conventional approaches deteriorates. The packet loss can be due to link errors or the combined effect of malicious and the link error. The above figure represents the combined effect of link and malicious errors.

III.PROPOSED SYSTEM

The related work on the detection of packet dropping attacks can be classified into two categories.

A. The first category aims at high malicious dropping rates, where most (or all) lost packets are caused by malicious dropping. In this case, the impact of link errors is ignored.

Most related work falls into this category. Based on the methodology used to identify the attacking nodes, these works can be further classified into four sub-categories. The first sub-category is based on credit systems. A credit system provides an incentive for cooperation. A node receives credit by relaying packets for others, and uses its credit to send its own packets. As a result, a maliciously node that continuous to drop packets will eventually deplete its credit, and will not be able to send its own traffic. The second sub-category is based on reputation systems. A reputation system relies on neighbors to monitor and identify misbehaving nodes. A node with a high packet dropping rate is given a bad reputation by its

neighbors. This reputation information is propagated periodically throughout the network and is used as an important metric in selecting routes. Consequently, a malicious node will be excluded from any route. The third sub-category of works relies on end-to-end or hop-to-hop acknowledgements to directly locate the hops where packets are lost. A hop of high packet loss rate will be excluded from the route.

B. The second category aims at the scenario where the number of maliciously dropped packets is higher than that caused by link errors, but the influence of link errors is non-negligible.

A. Disadvantages:

1) For the credit-system-based method, a malicious node may still receive enough credits by relaying most of the packets it receives from upstream nodes.

2) In the reputation-based approach, the malicious node can maintain a reasonably good reputation by forwarding most of the packets to the next hop.

3) For the acknowledgement-based method and all the mechanisms in the second category, counting the number of lost packets does not give a sufficient ground to detect the real attacker that is causing packet losse

IV. IMPLEMENTATION

In dropping data packet attack and routing packet attack malicious node prevents packets to forward to other mobile nodes and then drop these packets. One of the basic assumptions for the design of routing protocols in MANETs is that every node is equally important and cooperative. That means, if a node claims it can reach another node by a certain path or distance, then protocol takes the claim as real and similarly, when a node reports a link break, the link will not be used for next transmission. AODV is the commonly used reactive routing protocol in MANET. It is an on-demand protocol, which initiate route request only when needed. AODV is also affected by packet dropping attack. AODV performs better comparing to another protocol like dynamic source routing protocol (DSR) [13]. The proposed work adds security features to AODV and has introduced protocol named SAODV. Here it basically deals with packet dropping in network layer. The first level of acknowledgment, such as Transmission Control Protocol Acknowledgment can detect end-to-end communication break, it is unable to identify accurately the malicious node which contributes that attack. Such mechanism is unavailable for connectionless transport layer protocols like User Datagram Protocol. Therefore, securing the basic operation of the MANET becomes one of the primary concerns in mobile environments in the presence of packets droppers [2]. The challenge lies in securing communication with the maintenance of connectivity between nodes under the crucial attacking situations and the frequently changing topology.

Packet Dropping Attack In AODV

A malicious node involved in a routing path may intentionally drop the packets at network layer in order to make a collapse in network performances. If particular malicious node intentionally drops all the forwarded packets going through that node it can be termed as black hole attack. Here it may also occur selective packet dropping, in this attack malicious node can selectively drop the packets originated from or destined to certain nodes that it not likes [4].

Detecting selective packet-dropping attacks is more challenging in a highly mobile wireless environment. The main difficulty is the requirement that need not to only detect the node where the packet is dropped, but also identify whether the drop is intentional or unintentional. In order to precede a black hole attack, malicious node exploits the vulnerabilities of the AODV protocols which

V.RESULTS

Multiple users are created at a centralized location for the data owners and data users. We can see that either of the users can access the system once they login. The exchange of communication between data owners and data users is strictly through E-mail system which enables the system to be secured. Since the contents are encrypted and kept in the cloud, public viewing of these files is impossible. The files or contents can be viewed only after the consent of the data owners, after getting the secret key.

VI.CONCLUSION AND FUTURE

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 simulated with AODV and another with SAODV. From this experiment it is identified that routing complexity of SAODV is higher than AODV, but proper detection of 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. Detecting malicious packet dropping is a crucial issue in networks. The

conventional detection algorithms face several challenges that is best suited by the proposed approach. Exploiting the correlation between the lost packets improves the accuracy in detecting malicious packet drops. The truthfulness of the bitmap reported by each node is ensured by the cryptographic primitive which enables a public auditing architecture which is developed by HLA. This approach provides high detection accuracy. The randomized dispersive routes on detecting the malicious nodes effectively overcome the packet drop. To evaluate the performance of the proposed method, we simulated it using NS2. Experimental results relieved that proposed method performs well. Even though some open issues are to be considered in the future work. Changes in topology and link-characteristics are to be considered. In this paper we have assumed the source and destination are truthful, but malicious source and destination is a possibility which needs to be considered. The collaboration of nodes can also be exploited within the nodes to increase the efficiency of the routing path chosen. Hence a collaborative approach in detecting the malicious node based on the paper COCOWA can be applied as a future work.

.

REFERENCES

[1]. "Robust routing in wireless Ad hoc Networks", University of Maryland, 2002

[2]. R. Rao and G. Kesidis, "Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited," in Proc. IEEE GLOBECOM Conf., 2003.

[3]. K. Balakrishnan, J. Deng, and P. K. Varshney,

[4]. "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005.

[5]. K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgement-based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2006.

[6]. G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. Int. Conf. Theory Appl.Cryptol. Inf. Security, 2009

[7]. W. Kozma Jr. and L. Lazos, "Dealing with liars: Misbehavior identification via Renyi-Ulam games," presented at the Int. ICST Conf. Security Privacy in Commun. Networks, Athens, Greece, 2009.

[8]. W. Kozma Jr., and L. Lazos, "REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. ACM Conf. Wireless Netw. Secur., 2009

[9]. "Malicious Node detection for mobile ad hoc networks",International Journal of computer science, vol 2, 2010

[10]. Shu.T, Krunz.M, and Liu.S, "Secure data collection in wireless sensor networks using randomized dispersive routes". Vol. 9 no. 7, pp. 941–954, Mar 2010.

[11]. Wang.C, Wang.Q, Ren.K, and Lou.W. "Privacy-preserving public auditing for data storage security in cloud computing", Mar. 2010.

[12]. Proano.A and Lazos.L "Packet-hiding methods for preventing selective jamming attacks" Dependable and Secure Computing., vol. 9, no. 1, pp. 101–114, Aug 2012.

[13]. Amutha.S, Balasubramanian.K, "Secure Implementation ofRouting Protocols for Wireless Ad hoc Networks" pp. 960-965, Feb 2013.

[14]. "Secure routing and attack detection in wireless ad hoc network",vol 1, oct 2014

[15]. Tao Shu and Marwan Krunz "Privacy-Preserving and truthful Detection of packet dropping attacks in wireless ad hoc networks", vol 14, no. 4 April 2015

[16] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple cheat-proof, credit-based system for mobile ad-hoc networks," in Proc. IEEE INFO COM Conf., 2003, pp. 1987–1997.

[17] The MD5 Message-Digest Algorithm, RFC1321.