Volume No:2, Issue No:5 (October-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Privacy-Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks

Ch.Ramesh Kumar
Associate Professor & HOD,
Department of CSE,
Malla Reddy Engineering College & Management Sciences, Kistapur, Medchal, Hyderabad.

B. Prasanna Jyothi
Assistant Professor,
Department of CSE,
Malla Reddy Engineering College & Management Sciences, Kistapur, Medchal, Hyderabad.

Yedla Hemalatha
M.Tech Student,
Department of CSE,
Malla Reddy Engineering College & Management Sciences, Kistapur, Medchal, Hyderabad.

ABSTRACT:

Multi-hop wireless ad-hoc network (WANET) gives increase in coverage and provide more beneficiary over traditional wireless local area networks. However this architecture is more vulnerable in dealing with attacks internally from nodes which are compromised. One of them is packet dropping attack which is a very considerable in issue of networking. Link error and malicious packet dropping are two sources for packet losses. While observing a continuous packet loss in the network, it's hard to identify whether the loss is due to link errors or malicious ones. This research paper focuses on insider-attack scenario, whereby malicious nodes that are part of the route selectively drop a little amount of packets which are essential to the performance of the network. The malicious node may identify the importance of different packets and drops few of them which are important to the network operation. Since packet dropping rate in this case is comparable to the channel error rate, existing detection algorithms cannot achieve satisfactory detection accuracy in identifying packet loss rate. Improvement in Detection accuracy can be done by exploiting the correlations among packets lost. In this research paper, a public auditing is applied which allows the detector to find the truth about the packet loss information. The proposed technique is preserves privacy, collusion proof, and it incurs low communication and storage overheads at intermediate nodes. And also achieves better detection accuracy than the conventional methods such as a maximum likely detection.

KEYWORDS:

Packet Dropping, Auditing, Attack Detection, Secure Routing, truthfulness in packet drops, accurate detection of packet drops, wanet packet drop detection.

INTRODUCTION:

In a multi-hop network, nodes will cooperate in relaying/ routing traffic. An adversary can exploit this cooperative nature to do attacks. As an example, the adversary will first pretend to be a cooperative node in the route discovery method. Once entered in a route, the adversary node starts dropping packets. In the most severe form, the malicious node will stop forwarding all packets that receives from upstream nodes, completely disrupting the path between the source and destination. Actually, such a strong Denial-of-Service (DoS) attack can paralyze the network by partitions the topology. There are various reasons for packet losing which is shown in fig.1. A malicious node that is part of the route will explore its knowledge about the network policy and the communication context to launch an insider attack–which is intermittent, but can have similar performance degradation effect as a persistent attack at a much lower risk detecting frequently. Eventually, the malicious node can evaluate the importance of various packets, and then drop the little amounts that are highly critical to the operation of the network. For example, in a frequency-hopping network, those are the packets that express frequency hopping sequences for network-wide frequency-hopping synchronization; in an ad hoc radio network, they may be the packets that carry the idle channel lists (i.e., white spaces) which are used in establishment of a network-wide channel control. By targeting these highly critical packets, intermittent insider attacks may cause considerable damage for network with low probability of being caught. In this paper, we are enthusiastic to defend such insider attacks. In particular, we are interested in the problem of detecting the occurrence of selected packet droppings and identify the malicious node which is responsible for these drops.

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

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

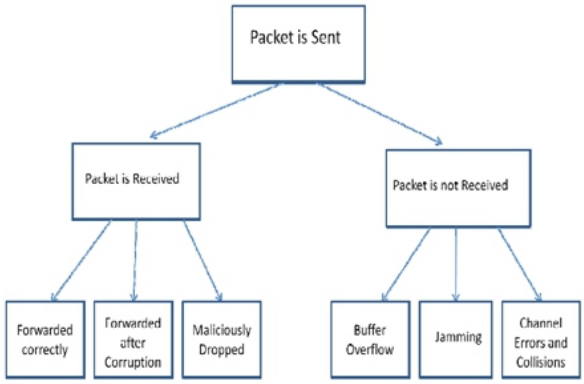

Fig. 1: Overview of Packet Loss

II. LITERATURE SURVEY:

In the year 2003 Borzoo Shadpour, Shahrokh Valaee, Baochun Li proposed paper titled "A Self-Organized Approach for Stimulating Cooperation in Mobile Ad Hoc Network" which contain the self-organized mechanism that is broke service, which allows for a broke node to use the network to transmit its traffic, in addition it providing an incentive to stimulate non-broke nodes to cooperate with broke ones. The main idea is to improve the connectivity of broke nodes in a pure ad-hoc networks. The proposed solution is loaning, which is interesting since it can be performed 'on-the-fly' by the nodes systems, and is suitable for the conditions of ad-hoc networks since it allows for nodes to remain self-organized. This scheme stimulates nodes to actively participate in the network, allowing the broke nodes to experience less delay when urgent transmission is desired. In the year 2005 Wenyuan XU, Wade Trappe, Yanyoung Zhang, Timothy Wood proposed a paper titled "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Network" which examine radio interference attacks from both sides of the issue: first, study the problem of conducting radio interference attacks on wireless networks, and second examine the critical issue of diagnosing the presence of jamming attacks. Specifically, proposes four different jamming attack models that can be used by an adversary to disable the operation of a wireless network, and evaluate their effectiveness in terms of how each method affects the ability of a wireless node to send and receive packets.

The paper also study different measurements that serve as the basis for detecting a jamming attack, and explore scenarios where each measurement by itself is not enough to reliably classify the presence of a jamming attack. In particular the signal strength and carrier sensing time are unable to conclusively detect the presence of a jammer. The paper proposes two enhanced detection protocols that employ consistency checking. The first scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, while the second scheme employs location information to serve as the consistency check. In the paper the feasibility and effectiveness of jamming attacks and detection schemes using the MICA2 Mote platform. In the year 2007 Jakob Erikson, Michalis Faloutsos, Srikanth V, Krishnamurthy proposed a paper titled "Routing amid Colluding Attackers "with the first practical solution to the long-standing problem of secure wireless routing in the presence of colluding attackers. The secure routing protocol, Sprout1, continuously tries new routes to the destination. Routes are generated probabilistically, with complete disregard for performance metrics. This nature makes Sprout uniquely resilient to attack. it cannot be tempted by any kinds of shortcuts. To avoid compromised routes, and to ensure good overall performance, the quality of each active route is monitored by means of signed end-to-end acknowledgments.

Based on this end-to-end acknowledgments amount of traffic sent on each route is adjusted accordingly. The vast majority of known routing layer attacks is mitigated by Sprout effectively, even when under assault from a large number of colluding attackers. . Sprout consistently delivers high, reliable performance in benign as well as hostile environments. In the year 2009 William Kozma Jr , Loukas Lazos proposed a paper titled "REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Network based on Random Audits" the paper investigate the problem of uniquely identifying the set of misbehaving nodes who refuse to forward packets. The resource-efficient account- ability for node misbehavior is identified by the new misbehavior identification scheme called REAct. The identification of misbehaving nodes based on a series of random audits triggered upon a performance drop is done in REAct. The source-destination pair using REAct can identify any number of independently misbehaving nodes based on behavioral proofs provided by nodes.

Volume No:2, Issue No:5 (October-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Proofs are constructed using Bloom filters which are storage efficient membership structures, thus significantly reducing the communication overhead for misbehavior detection. REAct has three phases (a) the audit phase (b) the search phase (c) the identification phase.

PROBLEM STATEMENT:

Detection of selected packet-dropping attacks is widely challenging in a highly dynamic environment. The hardness will be from the requirement that we need to not only detect the place of packet drop, but also find that the drop is intentional or unintentional. Specifically, due to the openness of wireless source, the packet drop in the network could be caused by rough channel conditions (e.g., fade, noise and interfering, link error), or by the insider attacker. In an open wireless environment, link errors are important, and will not be significantly smaller than the packet dropping rate of the insider attacker. Here the detection must be done by the public auditor that does not have knowledge of the data held by the nodes on the network route. When a malicious node is identified, the auditor should be able to construct a proof of the misbehavior of that node.

RELATED WORK:

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

A.The first one aims at huge malicious dropping rates, where most (or all) lost packets are caused by malicious droppings. The impact of link errors is ignored in this case. Most related work falls into this category. Based on the methods used to find the attackers, these works can be further classified into four sub-categories. The first one is on credit systems. A credit system provides an incentive for cooperation. A node receives credit on relay of packets, and uses that credit to send its own packets. As a result, a maliciously node that continuously drop packets that eventually deplete its credit, and will not be able to send its own traffic. The second one is on reputation systems. A reputation system relies on neighbors to monitor and identify misbehaving ones. The node with a high packet dropping rate is founded with a bad reputation by its neighbors. This reputation information is transmitted in periodical fashion throughout the network and is used as an important metric in selecting routes. Sequentially, a malicious one will be removed from any route.

The third sub-category of works relies on end-to-end acknowledgement that directly locates the hops where packets are lost. A hop of high packet loss rate will be excluded from the route.packets dropped by link errors, but the influence of link errors is non-negligible.

Limitations:

1) In the credit-system-based method, a malicious node may still receive enough credits by relaying most of the packets that received from up nodes.
2) The reputation approach, the malicious node can maintain a reasonably good reputation by sending much more packets to the next hop.
3) For the acknowledgement-based method and all the mechanisms in the second scheme, counting of lost packets does not give a sufficient ground to detect the real attacker causing packet loss.

V. PROPOSED SYSTEM:

The proposed method is based on detecting the correlations among the loosed packets over every hop in the path. It gives a truthful and publicly verifiable decision statistical analysis as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations among the positions of lost data, as calculated by the autocorrelation function (ACF) which describes the status of every packet in continuous of packet transmission. Therefore, by detecting the correlations between the lost packet, which can decide the reason for the packet loss is purely due to link errors, or is a combined effect of malicious drop and link error.

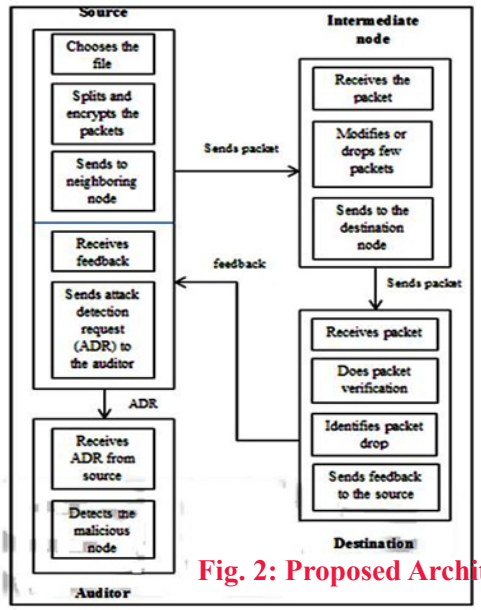

Fig. 2: Proposed Architecture

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

1IMPLEMENTATION

Network Configuration:

In this project we are using Wireless Ad hoc Network. Here we mainly focus on static or quasi-static network. In wireless network we need to send the packet through the node. System is represented as a node. Here every node has communication range. By using this range only we can transmit over packet. If source and destination node exists within the communication range, source can directly transmit the packet. Otherwise, we need to select the intermediate node based on the transmission range for transmit the packets.

Homomarphic Linear Authenticator:

To correctly calculate the correlation between lost packets, it is critical to enforce a truthful packet-loss bitmap report by each node. We use HLA cryptographic primitive for this purpose. The basic idea of our method is as follows. An HLA scheme allows the source, which has knowledge of the HLA secret key, to generate HLA signatures s1, . . , sM for M independent messages r1, . . . , rM, respectively. The HLA signatures are made in such a way that they can be used as the basis to construct a valid HLA signature for any arbitrary linear combination of the messages, , without the use of the HLA secret key, where ci's are randomly chosen coefficients. A valid HLA signature for , can be constructed by a node that does not have knowledge of the secret HLA key if and only if the node has full knowledge of s1, . . . , sM. So, if a node with no knowledge of the HLA secret key provides a valid signature for „ it implies that this node must have received all the signatures s1, . . . , sM.

Setup Phase and Packet Transmission Phase:

This phase takes place right after route PSD is established, but before any data packets are transmitted over the route. In this phase, S decides on a symmetric-key crypto-system (encrypt key, decrypt key) and K symmetric keys key1, . . . , keyK, where encrypt key and decrypt key are the keyed encryption and decryption functions, respectively. S securely distributes decrypt key and a symmetric key keyj to node nj on PSD, for j = 1, . . . ,K. Key distribution may be based on the public-key crypto-system such as RSA: S encrypts keyj using the public key of node nj and sends the cipher text to nj . nj decrypts the cipher text using its private key to obtain keyj .

After completing the setup phase, S enters the packet transmission phase. Before sending out a packet Pi, where i is a sequence number that uniquely identifies Pi, S computes ri = H1(Pi) and generates the HLA signatures of ri for node nj , as follows sji = [H2(i||j)uri]x, for j = 1, . . . ,K where || denotes concatenation. These signatures are then sent together with Pi to the route by using a one-way chained encryption that prevents an upstream node from deciphering the signatures intended for downstream nodes.

Audit Phase and Detecting 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 sequence numbers 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. 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.

CONCLUSION:

It is compared with conventional detecting algorithms which uses only the distribution of the number of lost packets, exploiting the correlation among lost packets drastically improves the accuracy in detecting malicious packet drops. Such improvement is highlighted if the count of maliciously dropped packets is comparable with those caused by link errors. To exact calculation of the correlation among lost packets, it is critical to acquire truthful packet-loss information at every individual node. Created a Public auditing system which ensures truthful packet-loss reporting by individual nodes. This architecture is proven collusion proof, which requires high computational capacity at the source node, which incurs in low communication and storage overhead in the route.

Volume No:2, Issue No:5 (October-2016) ISSN No : 2454-423X (Online)

International Journal of Research in Advanced Computer Science Engineering

A Peer Reviewed Open Access International Journal

www.ijracse.com

REFERENCES:

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

[2] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. ACM Conf. Comput. and Commun. Secur., Oct. 2007, pp. 598–610.

[3] 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.

[4] 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.

[5] 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.

[6] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.

[7] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the weil pairing," J. Cryptol., vol. 17, no. 4, pp. 297–319, Sep. 2004.

[8] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw. Comput. Conf., 2002, pp. 226–236.

[9] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in selforganizing mobile ad hoc networks," ACM/ Kluwer Mobile Netw. Appl., vol. 8, no. 5, pp. 579–592, Oct. 2003.

[10] J. Crowcroft, R. Gibbens, F. Kelly, and S. Ostring, "Modelling incentives for collaboration in mobile ad hoc networks," presented at the First Workshop Modeling Optimization Mobile, Ad Hoc Wireless Netw., Sophia Antipolis, France, 2003.

[11] J. Eriksson, M. Faloutsos, and S. Krishnamurthy, "Routing amid colluding attackers," in Proc. IEEE Int. Conf. Netw. Protocols, 2007, pp. 184–193.

Authors Biography:

Yedla Hemalatha completed his B.Tech degree in aurora technological institute in 2014. She is pursuing M.Tech. in Computer Science & Engineering from Department of Computer Science & Engineering in Malla Reddy Engineering College & Management sciences, Kistapur, Medchal, Hyderabad. Affiliated to JNTUH, HYDERABAD, TELANGANA, India.. Her research interest include cloud, data mining, Big Data and networking.

B. Prasanna Jyothi, working as Assistant Professor, department of computer science and engineering, in Malla Reddy Engineering College & Management Sciences, Kistapur, Medchal ,Hyderabad. Affiliated to JNTUH, HYDERABAD, TELANGANA., India. Her research interests include data mining, computer networks.

Ch. Ramesh Kumar, working as Assoc. Prof & Head of the Department of Computer Science and Engineering in Malla Reddy Engineering College & Management Sciences, Kistapur, Medchal, Hyderabad. Affiliated to JNTUH, HYDERABAD, TELANGANA., India. he has several international publications to his credit. His research interests include Software reuse, Software performance, Software testing ,Data Mining and cloud computing.