International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

Malicious Detection of Packet Dropping in Wireless AdHoc Network

[1] N.Suman, [2] K.Srinivas, [3]P.Srinivas Rao
[1]M.Tech ,CSE, Jayamukhi Institute Of Technological Sciences,Warangal,India
[2]Assistant professor,CSE, Jayamukhi Institute Of Technological Sciences,Warangal,India
[3]Associate professor,CSE, Jayamukhi Institute Of Technological Sciences,Warangal,India

Abstract:

Link error and malicious packet dropping are two sources for packet losses in multi-hop wireless circumstantial network Packet dropping is common attacks occur in wireless circumstantial Network. This threat happens once the information is transmitted from one supply to destination. The attack is also classified into 2 sorts one is malicious packet dropping. And another one is link error. We tend to are particularly inquisitive about the insider-attack case, whereby malicious nodes that are part of the route exploit their data of the communication context to by selection drop alittle amount of packets important to the network performance. To improve the detection accuracy, we tend to propose to take advantage of the correlations between lost packets. This can be overcome by the planned theme by implementing Homomorphic Linear critic (HLA). it's the general public auditing theme to find the malicious node in WANET. HLA act like associate degree auditor to find the packet losing schemes within the network. the most advantage of this theme can firmly transmit the information in WANET. The packet dropping rate is reminiscent of the channel error rate, standard algorithms that ar supported detective work the packet loss rate cannot win satisfactory detection accuracy.

Key Terms: Packet Losses, Homomorphic Linear critic, public auditing.

I. Introduction:

In a multi-hop wireless network, nodes collaborate in relaying/ routing traffic. Associate in Nursing resister will exploit this cooperative nature to launch attacks. as an example, the adversary might initial fake to be a cooperative node in the route discovery method. Once being enclosed in a very route, the resister starts dropping packets. In the most severe type, the malicious node merely stops forwarding each packet received from upstream nodes, fully disrupting the trail between the source and also the destination. Eventually, such a severe denial-of-service (DoS) attack will paralyze the network by partitioning its topology. Albeit persistent packet dropping will effectively degrade the performance of the network, from the attacker's standpoint such Associate in Nursing ―always-on‖ attack has its disadvantages. First, the continual presence of very high packet loss rate at the malicious nodes makes this kind of attack straightforward to be detected. Second, once being detected, these attacks ar straightforward to mitigate. For example, just in case the attack is detected however the malicious nodes don't seem to be known, one will use the randomized multi-path routing algorithms to circumvent the black holes generated by the attack, probabilistically eliminating the attacker's threat. If the malicious nodes also are known, their threats are often completely eliminated by merely deleting these nodes from the network's routing table. A malicious node that is a part of the route will exploit its data of the network protocol and also the communication context to launch Associate in Nursing corporate executive attack—an attack that's intermittent, but are able to do an equivalent performance degradation effect as a persistent attack at a way lower risk of being detected. Specifically, the malicious node might evaluate the importance of varied packets, and then drop the little quantity that ar deemed extremely essential to the operation of the network. as an example, in a frequency-hopping network, these can be the packets that convey frequency hopping sequences for networkwide frequency-hopping synchronization; in a billboard hoc cognitive radio network, they might be the packets that carry the idle channel lists (i.e., white spaces) that are used to establish a network-wide management channel. By targeting these extremely essential packets, the authors have shown that an 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. Detecting selective packet-dropping attacks is extremely challenging in a highly dynamic wireless environment. The difficulty comes from the requirement that we need to not only detect the place (or hop) where the packet is dropped, but also identify whether the drop is intentional or unintentional.

The work is classified into two categories. First category is based on malicious node dropping the packet which works on detecting the malicious node that causes the discarding of packets. Detection accuracy of malicious node is done by four ways. Whenever a node sends a packet it will earn a point for transmitting a packet. The malicious node which continuously discards the packet will lose its point [7] [6] [1] ii) Each node is monitored by its neighbor node. So the misbehaving node is monitored by the neighbor node iii) malicious node place will be identified and removed from the network. iv) Some cryptographic method is used to have the record of forwarded packets. All this ways of identifying the malicious node have disadvantages and these methods will not be applicable when the packets are highly selective. If a basic access procedure is used, the sender depends on feedback from the receiver to determine the cause of packet loss. If a packet with a corrupted header is received, the receiver sends nothing and the sender will timeout and assumes that a collision occurred. If a packet with a correct header is received but the data part is corrupted, the receiver can recognize the sender and reply with a NAK frame. Here, the sender will assume that the packet was lost due to channel error.

II. Related Work:

T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim, Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks.

Detecting malicious packet dropping is important in ad hoc networks to combat a variety of security attacks such as blackhole, greyhole, and wormhole attacks. We consider the detection of malicious packet drops in the presence of collisions and channel errors and describe a method to distinguish between these types. We present a simple analytical model for packet loss that helps a monitoring node to detect malicious packet dropping attacks. The model is analyzed and evaluated using simulations. The results show that it is possible to detect malicious packet drops in the presence of collisions and channel errors.

G. Noubir and G. Lin, Low-power DoS attacks in data wireless lans and countermeasures.

In this paper we investigate the resiliency to jamming of data protocols, such as IP, over WLAN. We show that, on existing WLAN, an adversary can successfully jam data packets at a very low energy cost. Such attacks allow a set of adversary nodes disseminated over an area to prevent communication, partition an ad hoc network, or force packets to be routed over adversary chosen paths. The ratio of the jamming pulses duration to the transmission duration can be as low as 10--4. We investigate and analyze the performance of using various coding schemes to improve the robustness of wireless LANs for IP packets transmission. A concatenated code that is simple to decode and can maintain a low Frame Error Rate (FER) under a jamming effort ratio of 15%. We argue that LDPC codes will be very suitable to prevent this type of jamming. We investigate the theoretical limits by analyzing the performance derived from upper bounds on binary error-control codes. We also propose an efficient anti-jamming technique for IEEE802.11b.

P. Papadimitratos and Z. Haas, Secure message transmission in mobile ad hoc networks.

The vision of nomadic computing with its ubiquitous access has stimulated much interest in the mobile ad hoc networking (MANET) technology. However, its proliferation strongly depends on the availability of security provisions, among other factors. In the open, collaborative MANET environment, practically any node can maliciously or selfishly disrupt and deny communication of other nodes. In this paper, we propose the secure message transmission (SMT) protocol to safeguard the data transmission against arbitrary malicious behavior of network nodes. SMT is a lightweight, yet very effective, protocol that can

operate solely in an end-to-end manner. It exploits the redundancy of multi-path routing and adapts its operation to remain efficient and effective even in highly adverse environments. SMT is capable of delivering up to 83% more data messages than a protocol that does not secure the data transmission. Moreover, SMT achieves up to 65% lower end-to-end delays and up to 80% lower delay variability, compared with an alternative single-path protocol—a secure data forwarding protocol, which we term secure single path (SSP) protocol. Thus, SMT is better suited to support quality of service for real-time communications in the ad hoc networking environment. The security of data transmission is achieved without restrictive assumptions on the network nodes' trust and network membership, without the use of intrusion detection schemes, and at the expense of moderate multi-path transmission overhead only.

R. Rao and G. Kesidis, Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited.

Ad hoc networks are gaining presence with the proliferation of cheap wireless devices and the need to keep them connected. Individual applications and larger missions, such as those of tactical sensor networks, require secure data transmission among wireless devices. Security remains a major challenge for such networks. Current protocols employ encryption and authentication techniques for secure message exchange, but given the limitations and innately insecure nature of ad-hoc networks, such mechanisms may not suffice. A security breach can, for example, be a network-level denial-of-service (DoS) attack, passive eavesdropping, or physical layer jamming to degrade communication channels. In a multihop network, an intruder node can degrade communication quality by simply dropping packets that are meant to be relayed (forwarded). The network could then misinterpret the cause of packet loss as congestion instead of malicious activity. In this paper, we suggest that traffic transmission patterns be selected to facilitate verification by a receiver. Such traffic patterns are used in concert 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, e.g., certain kinds of tactical sensor networks.

C. Wang, Q. Wang, K. Ren, and W. Lou, Privacy-preserving public auditing for data storage security in cloud computing.

Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

III. System Model:

In this paper, we tend to develop associate degree correct algorithmic rule for detecting selective packet drops created by corporate executive attackers. Ourϖ algorithmic rule additionally provides a truthful and publically verifiable call statistics as a symbol to support the detection call. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation operate (ACF) of the packet-loss electronic image—a bitmap

describing the lost/received standing of every packet in an exceedingly sequence of consecutive packet transmissions. The basic idea behind this method is that even though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the stochastic processes that characterize the two phenomena exhibit different correlation structures (equivalently, different patterns of packet losses). Therefore, by detecting the correlations between lost packets, one can decide whether the packet loss is purely due to regular link errors, or is a combined effect of link error and malicious drop. Our algorithm takes into account the crossstatistics between lost packets to make a more informative decision, and thus is in sharp contrast to the conventional methods that rely only on the distribution of the number of lost packets. The proposed scheme requires relatively high computation capability at the source, but incurs low communication and storage overheads along the route. Most of the computation is done at the source node (for generating HLA signatures) and at the public auditor (for conducting the detection process). We consider the public auditor as a dedicated service provider that is not constrained by its computing capacity. So the computational overhead should not be a factor limiting the application of the algorithm at the public auditor. On the other hand, the proposed algorithm requires the source node to generate K HLA signatures for a K-hop path for each data packet. The generation of HLA signatures is computationally expensive, and may limit the applicability of the algorithm.

The communication overhead for the setup section may be a one-time price, incurred once PSD is established. Here we tend to primarily specialize in the revenant price throughout the packet transmission and auditing phases (there isn't any communication overhead within the detection phase). For a transmitted packet P_i, S has to send one encrypted HLA signature and one mackintosh to every intermediate node on PSD. Our HLA signature follows the BLS theme in . thus associate degree HLA signature s_{ij} is 160-bit long. If encrypted by DES, the encrypted signature s_{ij} is 192 bits long (a block in DES is 64- bit long, that the length of the cipher text of DES is multiples of sixty four bits). The MAC-related hash operate HkeyMAC are often enforced in SHA-1 and encompasses a length of 160 bits. Thus for every packet, the per-hop communication overhead incurred by the projected theme within the packet transmission section is 192 þ 160 ¼ 352 bits, or 44 bytes. For a path of K intermediate hops, the whole communication overhead for sending a packet is 44K bytes.

IV. Conclusion:

In this paper, we tend to showed that compared with conventional detection algorithms that utilize solely the distribution of the amount of lost packets, exploiting the correlation between lost packets considerably improves the accuracy in police work malicious packet drops. Such improvement is particularly visible once the number of maliciously born packets is comparable with those caused by link errors. to properly calculate the correlation between lost packets, it's vital to acquire truthful packet-loss info at individual nodes. we tend to developed associate HLA-based public auditing architecture that ensures truthful packet-loss news by individual nodes. This design is collusion proof, needs comparatively high machine 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 additionally planned, which permits one to trade detection accuracy for lower computation quality. Some open problems stay to be explored in our future work. First, the planned mechanisms are restricted to static or quasi-static wireless accidental networks. Frequent changes on topology and link characteristics haven't been considered.

References:

[1] T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim, "Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks," in Proc. IEEE Int. Conf. Commun., 2009, pp. 1062–1067.

[2] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless lans and countermeasures," ACM SIGMOBILE Mobile Comput.Commun. Rev., vol. 7, no. 3, pp. 29–30, Jul. 2003.

[3] V. N. Padmanabhan and D. R. Simon, "Secure traceroute to detect faulty or malicious routing," in Proc. ACM SIGCOMM Conf., 2003,pp. 77–82.

[4] P. Papadimitratos and Z. Haas, "Secure message transmission in mobile ad hoc networks," Ad Hoc Netw., vol. 1, no. 1, pp. 193–209,2003.

[5]A. Proano and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks," IEEE Trans. Depend. Secure Comput.,vol. 9, no. 1, pp. 101–114, Jan./Feb. 2012.

[6]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, pp. 2957–2961.

[7]C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM Conf., Mar. 2010, pp. 1–9.

[8]W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. ACM MobiHoc Conf., 2005, pp. 46–57.

[9]T. Shu, M. Krunz, and S. Liu, "Secure data collection in wireless sensor networks using randomized dispersive routes," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[10] T. Shu, S. Liu, and M. Krunz, "Secure data collection in wireless sensor networks using randomized dispersive routes," in Proc. IEEE INFOCOM Conf., 2009, pp. 2846–2850.