ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Packet Classification Methods to Counter Jamming Attacks in Adhoc Networks

P.Ramesh Kumar [1], G.Nageswara Rao [2], P.Rambabu [3]

[1]Sasi Institute of Technology and Engineering, Tadepalligudem,W.G(dt)

[2] Assoc professor, Sasi Institute of Technology and Engineering,Tadepalligudem,W.G(dt)

[3]Assoc.professor, HOD, Sasi Institute of Technology and Engineering, Tadepalligudem,W.G(dt)

Abstract:

Jamming attacks though is not a new phenomenon leads to disruptions in the communications channel which is a serious concern in Reactive protocols driven Adhoc networks. The jamming models are categorised as both external and internal with the later being more serious nature because the "always-on" strategy employed in external model has several risk factors to the jammer's identity. External model involves the jammer spending a significant amount of energy to jam frequency bands of interest. The continuous presence of these unusually high interference levels makes this type of attacks easy to detect. In an internal threat model a jammer is assumed to be aware of network details and the implementation details of network protocols at any layer in the network stack. The jammer exploits his internal knowledge for launching selective jamming attacks in which specific packets of "high priority" are targeted. Although RREQ,RREP,RERR, RREP-ACK are primary Message Formats in reactive protocols, the adversary selectively targets RREQ and RREP packets in the network to launch jamming attacks. Existing approaches concentrated on using commitment schemes that are cryptographic primitives to hide the RREQ and RREP packets from the purview of the adversary. These approaches being successful, we propose to use them along with intrusion detection techniques for identifying compromised access points to increase overall network security significantly by marginalizing the working boundaries of an adversary, thus risking exposure. A resultant network prototype validates our claim.

Keywords—Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification.

I INTRODUCTION

Ad hoc networks are an integral part in mission critical communication for the military, utilities, and industry. An adversary may attempt to attack a victim ad hoc network to prevent or hijack some or all of the victim's communication. Such attacks have been considered as potential threats in ad hoc wireless networks at several levels. A number of researchers have considered DoS where the attackers are internal participants in the victim ad hoc network (see e.g. [1]). Internal threat model of Ad hoc networks requires the cooperation of participant nodes for their operation and are especially susceptible to such peer based attacks.

In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated jammer who is aware of network configurations and the implementation details of network protocols at any layer in the network stack. The jammer exploits his internal knowledge for launching selective jamming attacks in which specific packets of "high importance" such as RREQ and RREP are targeted [9]. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow.

To launch selective jamming attacks, the attacker must be capable of implementing the "find-then-jam"

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

strategy before or during the the completion of a wireless transmission. Such strategy can be realized either by classifying transmitted packets using network stack based protocol semantics [5], [6], or by decoding packets on the fly [7]. In the latter method, the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the attacker must introduce a significant number of bit errors so that the packet cannot be recovered at the receiver [8]. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

Jamming can be as simple as sending out a strong noise signal in order to prevent packets in the victim network from being received. This method of jamming is not the subject of this paper. This paper attempts to exploit the protocols at various layers to get three advantages: jamming gain; targeted jamming; and reduced probability of detection. Jamming gain is the increase in efficiency from exploiting features of the victim network relative to continuous jamming. More precisely, it is the amount of energy (or power as appropriate) used to achieve a desired effect relative to the amount of energy used to achieve the same effect with continuous jamming. This gain translates directly into reduced energy requirements for the attacker. At the link level, corrupting a single bit in a packet will cause the packet to fail its checksum and be discarded. For a 10,000 bit packet (1250 bytes) it implies that jamming gains as high as 40dB are possible. Further, typical wireless packet networks are lightly loaded so that jamming only when packets are present has further jamming gains. These examples make clear that there are significant jamming gains possible. This concept can be fully explored later in future research.

Targeted jamming refers to jamming only specific victim nodes or packets, links, or flows. The attacker may be interested in only certain parts of the victim network, and attacking only these parts can lead to further jamming gains. With reduced probability of detection, the victim network may not realize that jamming countermeasures are necessary. Targeting some TCP-DATA packets will cause the TCP window to collapse and poor connection performance that a user might attribute to network congestion or a low quality wireless connection. Further, if ICMP packets are not blocked the victim users will have contradictory views of the network state. If jamming is discovered, lower probability of detection jamming will be harder to detect, localize, and suppress.

Jamming is not a transmit-only activity. It requires an ability to detect and identify victim network activity, which we denote as sensing. At the physical layer a sensor needs to identify the presence of packets. Since the network is encrypted, only the start time and size of the packet can be measured. At higher layers a sensor needs to classify packets using protocol information. In 802.11 for instance, whether a packet is successfully jammed or not can be seen by whether or not a node sends a short packet (i.e. the ACK) within 10μsec.

II RELATED WORK

In this Chapter, references of previous research that utilized the concepts in Introduction are introduced. For each of the concepts, an overview of related literature is provided. In Section A, WLAN is introduced. Specifically, client-server and ad-hoc networks are explained. In Section B, DoS attacks, especially jamming attacks are presented. In Section C, detection methods of jamming attacks are analyzed.

Section A. WLAN – Client-Server & Ad-Hoc Network Because WLAN provides users the mobility to move around within a local area without a wire and still connect to the network, it is widely used in many important areas. Banks, governments, corporations, and institutions transmit highly important data through WLANs. The security problems of WLANs become important for the users.Most WLANs are based on the IEEE 802.11 standard, which transmits data in different channels based on frequencies. Due to the ease of installation and convenience, WLAN is regularly used in daily life. An introduction of WLANs was done by Gast (2005) and Mark (2005). They presented basic wireless LAN technology, why the technology had

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

emerged, how it works, the architecture of WLANs, and the types of WLANs.Because of the popularity of WLANs, security research must be done in various types of WLANs. Experiments were done by Varadarajan , Kumar, and Reddy (2011) about improving WLAN performance under DoS attacks. DoS attacks on the physical layer were analyzed and expanded to the security of the physical layer of the sensor network model. This research was done by using the ant system. By using Receiver Operating Characteristics (ROC) on nodes, DoS 8 attacks can be predicted by formulating the classification of jammers under various attack scenarios. This approach can help improving detecting DoS attacks in WLANs.Research in this thesis was focuses on two types of WLANs: client-server and ad-hoc networks.

Section B. Jamming Attacks The DNS is a hierarchical tree structure whose root node is known as the root domain. A label in a DNS name directly corresponds with a node in the DNS tree structure. A label is an alphanumeric string that uniquely identifies that node from its brothers. Labels are connected together with a dot notation, ".", and a DNS name containing multiple labels represents its path along the tree to the root. Labels are written from left to right. Only one zero length label is allowed and is reserved for the root of the tree. This is commonly referred to as the root zone. Due to the root label being zero length, all FQDNs end in a dot [RFC 1034].A study into DoS attacks and defense was done by Raymond and Midkiff (2008). Since WSNs are used in monitoring medical uses, homeland security, industrial automation, and military applications, security of WSNs must be guaranteed. Defeating many threats of DoS attacks on WSNs can be done by encryption and authentication, but some other techniques still need to be found to prevent from special DoS attacks, especially Denial of Sleep attacks, which are still critical threats in WSNs.

Section C. Detection of Jamming WLANs are built upon a shared medium that makes it easy to launch jamming attacks. These attacks can be easily accomplished by sending radio frequency signals that do not follow any MAC protocols. Detection of jamming attacks can be done in multiple ways. One of the most efficient ways is to jump channels. Because communication between two legitimate nodes is done through a specific frequency, the frequency can be changed if necessary. While a jammer is attacking the wireless network, there are other effective ways to continue legitimate communication in the network. Engaging the jammer on the jammed channel and continuing communication in another channel was introduced by Beg, Ahsan, and Mohsin (2010). When the nodes detected the jamming in the wireless network, they jumped to another channel to continue legitimate communication. In the experiments, both 10 and 20 nodes experiments were done, and in both scenarios, after channels were jumped, the network resumes communications as normal. In both scenarios, the amount of packets dropped reduced immediately. The research concluded that channel jumping will decrease the throughput of the network. Also, it was easier to detect jamming through intermitted channel jumping. Concluded, channel jumping was a superior method of combating network interference, rather than changing network protocols (Jeung, Jeong, and Lim, 2011).The research concluded that channel jumping will decrease the throughput of the network. Also, it was easier to detect jamming through intermitted channel jumping. Concluded, channel jumping was a superior method of combating network interference, rather than changing network protocols (Jeung, Jeong, and Lim, 2011).In order to prevent from multi-channel jamming attacks, a cross-layer jamming detection method was developed (Chiang and Hu, 2011). Cross-layer jamming detection is a tree-based approach. A jamming detection algorithm was utilized in all legitimate nodes; when the communication process began, all the nodes had the ability to report jamming attacks in different layers, and only the reports which were generated by nodes with jamming detection algorithm were accepted by the system in order to avoid error. Research was also done about multi-channel jamming attacks by Jiang and Xue (2010). The difference from the jamming detection algorithm was that it focused on network restoration and design of traffic rerouting.

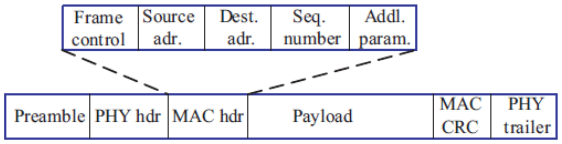
ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

III PRELIMINARIES

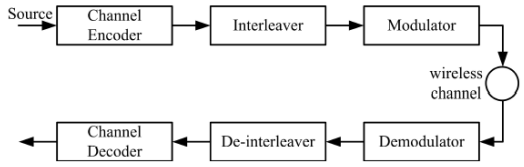
The following lists basic terminologies required for understanding of Adhoc network implementations.

Sequence Name	Packets in Sequence
Data-Ack	TCP-DATA, TCP-ACK
ARP	ARP-REQ, ARP-RESP
TCP-Startup	TCP-SYN, TCP-SYN-ACK, TCP-ACK
AODV	AODV-RREQ, AODV-RREP(unicast)
DNS-Lookup	UDP-DATA, UDP-DATA

The types of packet sequences are shown in the following table.



A Typical Packet Frame Format in a Mobile Adhoc Network



PHY layer communication system diagram

IV AONT-based Hiding Scheme

1. Symmetric encryption algorithm
2. Brute force attacks against block encryption algorithms.

We propose a solution based on All-Or- Nothing Transformations (AONT) that introduces a modest communication and computation overhead. Such transformations were originally proposed by Rivest to slow down brute force attacks against block encryption algorithms . An AONT serves as a publicly known and completely invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm

Algorithm Description

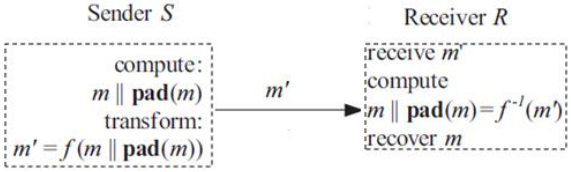


Fig- 1 : The AONT-based Hiding Scheme (AONT-HS)

The Package Transform- In the package transform ,given a message m, and a random key k′, the output pseudo-messages are computed as follows:

$$m'_i = m_i \oplus E_{k'}(i), \text{ for } i=1,2,3\ldots\ldots,x$$
$$m'_{x+1} = k' \oplus e_1 \oplus e_2 \oplus e_3 \oplus \ldots\ldots\ldots\ldots \oplus e_x,$$

Where ei = Ek0 (m'i ⊕i), for i = 1, 2, . . . , x, and k0 is a fixed publicly-known encryption key. With the reception of all pseudo-messages message m is recovered as follows:

$$k' = m'_{x+1} \oplus e_1 \oplus e_2 \oplus e_3 \oplus \ldots\ldots\ldots\ldots \oplus e_x,$$
$$m_i = m'_i \oplus E_{k'}(i), \text{ for } i=1,2,3\ldots\ldots,x,$$

Note that if any m'i is unknown, any value of k′ is possible, because the corresponding ei is not known. Hence, Ek' (i) cannot be recovered for any i, making it infeasible to obtain any of the mi .

Hiding Sublayer Details- AONT-HS is implemented at the hiding sublayer residing between the MAC and the PHY layers. In the first step, m is padded by applying function pad() to adjust the frame length so that no padding is needed at the PHY layer, and the length of m becomes a multiple of the length of the pseudo-messages m′ i. This will ensure that all bits of the transmitted packet are part of the AONT. In the next step, m||pad(m) is partitioned to x blocks, and the AONT f is applied. Message m′ is delivered to the PHY layer. At the receiver, the inverse transformation f−1 is applied to obtain m||pad(m). The padded bits are removed and the original message m is recovered. The steps of AONT-HS are shown in Fig. 1.

Node joining access point optimization to counter forced network joins

In the second phase the querying node propagates Ltotal to all nodes in the network, possibly by using the same hi-erarchy created in the LB phase. This requires only n – 1 messages, where n is the number of nodes in the network. Each node receiving Ltotal, searches its local sorted list(vi) in order to identify

ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

the index of the lowest ranked object that belongs to Ltotal. More precisely, a procedure Find-MinRank locates the lowest ranked object that belongs to Ltotal. All objects above idx are candidates for the result.

```
1: procedure FINDMINRANK(L_total, list(v_i))
2:     idx = −1
3:     for j = 1 to |L_total| do
4:         if (idx < rank(L_total[j], list(v_i)) then
5:             idx = rank(L_total[j], list(v_i))
6:         end if
7:     end for
8:     return idx
9: end procedure
```

In the next step, each node uses the locally generated idx in order to extract the top-idx from its sorted list(vi). Let listidx(vi) denote the set of oij pairs generated by this procedure. If a node is a leaf node, it simply forwards listidx(vi) towards its parent. Otherwise a node waits until it receives all listidx(vj) from one of its children vj , at which point it performs a full outer join using the FullOuterJoin procedure illustrated next. We note that in a full outer join of two re- lations A and B, in addition to the rows that join on the objectID, the rows of both A and B without a match also appear in the result. However, the rows that don't match in both A and B, are marked with a incomplete flag. Below we present how optimized Access Point initiated node joining works:

$$R(v_i) = list_{idx}(v_i) \biguplus \left(\biguplus_{\forall j \in children(v_i)} list_{idx}(v_j) \right)$$

The above procedure creates a local partial result R(vi). During this computation the algorithm computes a partial score for each object oj in R(vi). If object oj appears in the result list of vi and in the result list of all its children this partial score can be computed exactly using formula

V PERFORMANCE

We investigate the performance of the proposed detection mechanism by an extensive real time network application involving WLAN Access points and manet nodes. We consider the detailed network statistics obtained from our jamming sequence simulator framework. To simulate attacks, the jammer nodes are activated and introduced at varying locations after the ad hoc network starts operating, to allow the nodes to settle down into a steady state before the jamming starts, thereby simulating the attack scenario described in prior sections.

We setup a 1 Mbps IEEE 802.11 network with a two-ray ground propagation model at the physical layer. Simulations use CBR (Constant Bit Rate) application generating traffic of data packets of 512 bytes with an inter-arrival packet time of 2 packets per second. Simulation time is 900 seconds and each simulation is repeated 10 times for different seed values to obtain steady state performance metrics. We model the malicious nodes to perform one or more of the jamming attacks at the physical and MAC layers. Initially, a subset of nodes in the network is randomly pre-deployed as monitor nodes. Once the attack is initiated, the network subsequently follows reactive monitor selection to choose the monitors.

Fig 5 (a) Effect of Jammer Distance on Throughput loss

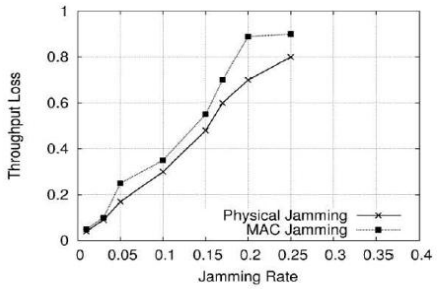


Fig 5 (b) Effect of Jammer Rate on Throughput loss

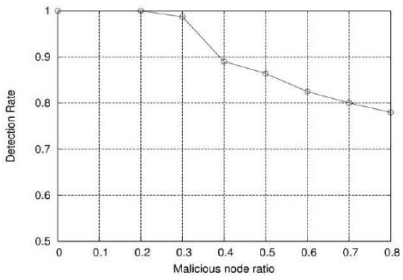
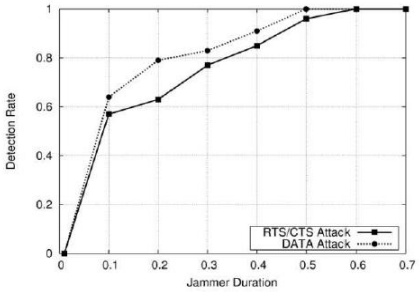


Fig 5 (c) Impact of malicious node ratio on detection rate



ISSN-2320-7884 (ONLINE)
ISSN-2321-0257 (PRINT)

Fig 5 (d) Impact of jamming duration on detection rates

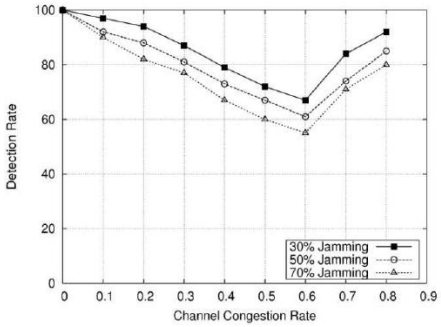


Fig 5 (e) Impact of channel congestion rate on detection rate

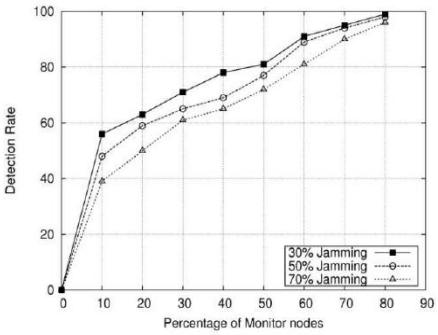


Fig 5 (f) Impact of monitor node ratio on detection rate

VI CONCLUSION

We addressed the problem of selective jamming attacks in adhoc networks in an internal threat model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network details. We showed that the jammer can classify transmitted packets at will in a real time network scenario by decoding the first few symbols of an ongoing transmission. We evaluated its impact of selective jamming attacks on network protocols such as TCP and routing. Our results show that a selective jammer can significantly impact performance with very low effort. We developed cryptographic primitives scheme that uses commitment schemes, cryptographic puzzles, and all-or-nothing transformations (AONTs) with physical layer characteristics. We analyzed the security of our schemes and quantified their computational and communication overhead. Th source of the problem lien in the Access point validation of the jammer which is addressed using the router Minrank strategy preventing Denial Of Service based authentication attempts of the jammer, thus improving the network conditions. As discussed in the introductory part jamming gain estimations do help to improve performance more which can be an interesting future research.

VIII REFERENCES

[1] Hu, Y.-C., Perrig, A. A survey of secure wireless ad hoc routing. IEEE Security & Privacy Magazine. v. 02, n. 3, (May–Jun.2004),pp. 28–39.

[2] T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.

[3] D. Thuente andM. Acharya. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In Proceedings of the IEEE Military Communications Conference MILCOM, 2006.

[4] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. Reactive jamming in wireless networks: How realistic is the threat? In Proceedings of WiSec, 2011.

[5] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based antijamming techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.

[6] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007.

[7] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper. Intelligent sensing and classification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.

[8] O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.

[9] Alejandro Proano and Loukas Lazos. Packet-Hiding Methods for Preventing Selective Jamming Attacks. IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING ,VOL. 9, NO. 1, JAN-FEB 2012