



AVERTING SELECTIVE JAMMING ATTACKS USING PACKET-HIDING TECHNIQUES

P. Vijayalaksmi

Research Scholar

Department of Computer Science

P.K.R. Arts College for Women

Gobichettipalayam, Tamil Nadu, INDIA

Abstract: The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages or jam legitimate ones. Typically, jamming has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. The problem of selective jamming attacks in wireless networks is to be considered as the key aspect during the packet delivered from source to destination. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. The advantages of selective jamming in terms of network performance degradation can be classified into two different types such as by selective attack on TCP and one on routing. Selective jamming attacks can be launched by performing real-time packet classification at the physical layer. Analysis of the security of the methods and evaluate their computational and communication overhead. Multiple-path source routing protocols allow a data source node to distribute the total traffic among available paths. Here the problem of jamming-aware source routing is concentrated and the source node performs traffic allocation based on empirical jamming statistics at individual network nodes. This traffic allocation is specified as a lossy network flow optimization problem using portfolio selection theory from financial statistics. In multi source networks, the centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization (NUM). The network's ability to estimate the impact of jamming and incorporate these estimated jamming into the traffic allocation problem. The throughput can be achieved using our proposed traffic allocation method in several scenarios. The jamming node information is gathered on the server side. On gathering the jamming node information from the client to the server then effective path table can be produced to the client node to transfer the data without jamming attack.

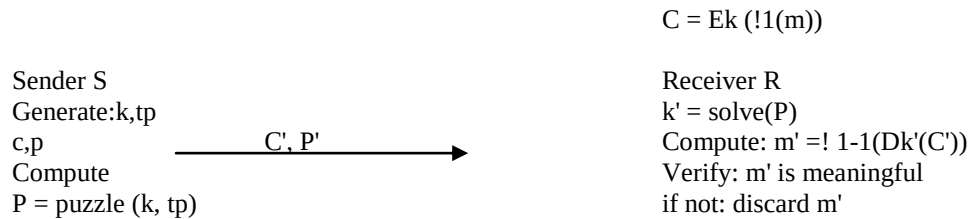
Keywords: Jamming, Routing, Multisource Networking, Network Utility Maximization

I. INTRODUCTION

The impact of an external selective jammer targets various control packets at the MAC layer. To perform packet classification, the adversary exploits inter-packet timing information to infer eminent packet transmissions. The proposed estimation of the probability distribution of inter-packet transmission times for different packet types based on network traffic analysis. Future transmissions at various layers were predicted using estimated timing information. The feasibility of selective jamming based on protocol semantics. They considered several packet identifiers for encrypted packets such as packet size, precise timing information of different protocols, and physical signal sensing. To prevent selectivity, the unification of packet characteristics such as the minimum length and inter-packet timing was proposed. A smart jammer that takes into account protocol specifics to optimize its jamming strategy. The adversary was assumed to target control messages at different layers of the network stack. To mitigate smart jamming the spread system, this is based on the idea of stochastic selection between collections of parallel protocols at each layer. The uncertainty introduced by this stochastic selection, mitigated the selective ability of the jammer. This protocol hides all explicit identifiers from the transmitted packets by encrypting them with keys only known to the intended receivers. Selective jamming attacks have been experimentally implemented using software-defined radio engines. To protect control-channel traffic, the replication of control transmission in multiple channels was suggested in the locations of control channels where cryptographically protected.

II. STUMBLING BLOCK ON SELECTIVE JAMMING

The packet hiding scheme is based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle to execute a pre-defined set of computations before the recipient is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of the puzzle-based scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation and communication overhead.



The Cryptographic Puzzle-Based Hiding Scheme

The cryptographic puzzles to temporarily hide transmitted packets. A packet m is encrypted with a randomly selected symmetric key k of a desirable length s . The key k is blinded using a cryptographic puzzle and sent to the receiver. For a computationally bounded adversary, the puzzle carrying k cannot be solved before the transmission of the encrypted version of m is completed and the puzzle is received. Hence, the adversary cannot classify m for the purpose of selective jamming. The problem of traffic allocations in multiple-path routing algorithms in the presence of jammers, whose effect can only be characterized statistically. Centralized protocols for source routing may be undesirable due to excessive communication overhead in large-scale wireless networks. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information. Path allocation for the Source node is done by the Server. Does not capture's the Jamming nodes details while assigning the Path for the source nodes. Network path having low bandwidth is not effectively used.

III. ANTICIPATED SYSTEM

The anticipated system is mainly based on the methods to defend a network against jamming attacks comprise physical layer solutions such as spread-spectrum. The sophisticated adversary, who is aware of network secrets implements details of the network protocols at any layer in the network stack. 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. The anti-jamming diversity based on the use of multiple routing paths, using multiple-path variants of source routing protocols such as Dynamic Source Routing (DSR) or Ad Hoc On-Demand Distance Vector (AODV). The presented methods for each network node to probabilistically characterize the local impact of a dynamic jamming attack and for data sources to incorporate this information into the routing algorithm. In general it allows the data sources to balance the expected data throughput with the uncertainty in achievable traffic rates. The centralized optimization problem can be solved using a distributed algorithm based on decomposition in Network Utility Maximization (NUM). In general it formulates the problem of allocating traffic across multiple routing paths in the presence of jamming as a lossy network flow optimization problem. To map the optimization problem to that of asset allocation using portfolio selection theory. The centralized traffic allocation problem for multiple source nodes as a convex optimization problem. To show that the multi-source multiple-path optimal traffic allocation can be computed at the source nodes using a distributed algorithm based on decomposition in network utility maximization (NUM). The proposed methods which allow individual network nodes to locally characterize the jamming impact and aggregate this information for the source nodes. The use of portfolio selection theory allows the data sources to balance the expected data throughput with the uncertainty in achievable traffic rates. Due to jamming at nodes along the path, the traffic rate is potentially reduced at each receiving node as packets are lost.

IV. PROBLEM DEFINITION

The packet transmission taken place from source to destination in a wireless communication in general the network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in unicast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using pre shared pair wise keys or asymmetric cryptography. Path allocation for the Source node is done by the Server. It does not capture's the Jamming nodes details while assigning the Path for the source nodes. Network path having low bandwidth is not effectively used. To overcome the selective jamming attacks during the packet transmission the portfolio selection of route in multi path transmission is done by the optimal route selection methods in which the path with the traffic are eliminated and the path without any disturbance are used to transmitted the packets using the portfolio selection theory by the threshold value. By this way the effective packet transmission are performed without any traffic in the networks.

V. PORTFOLIO SELECTION THEORY

Jamming has been addressed under an external threat model. However, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. The problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. This illustrates the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. These show, those selective jamming attacks can be launched by performing real-time packet classification at the physical layer. The security in these methods evaluate their computational and communication overhead. Multiple-path source routing protocols allow a data source node to distribute the total traffic among available paths. The problem of jamming-aware source routing in which the source node performs traffic allocation based on empirical jamming statistics at individual network nodes. This traffic allocation as a lossy network flow optimization problem using portfolio selection theory from financial statistics. This shows that in multi source networks, this centralized optimization problem can be solved using a distributed algorithm based on decomposition in network utility maximization (NUM). It demonstrates the network's ability to estimate the impact of jamming and incorporate these estimates into the traffic allocation problem. Finally, it simulates the achievable throughput using our proposed traffic allocation method in several scenarios. Gathering the Jamming node information on the server whereas, here it has done on the client side. On gathering this jamming node information from the client to server side it can produce an effective path table to the client node to transfer the data.

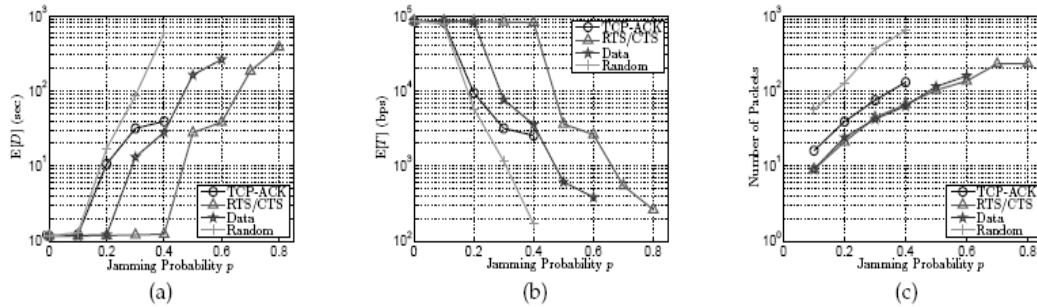
VI. THE PROCESS OF SELECTING A PORTFOLIO

This may be divided into two stages. The first stage starts with observation and experience and ends with beliefs about the future performances of available securities. The second stage starts with the relevant beliefs about future performances and ends with the choice of portfolio. The rule that the sender does (or should) maximize discounted expected, or anticipated, returns. This rule is rejected both as a hypothesis and as a maximum to guide sender behavior. The geometric relations between beliefs and choice of portfolio according to the "expected returns-variance of returns" rule. The nature of the set of efficient portfolios, it is not difficult to see the nature of the set of efficient (E, V) combinations. In the three security case $E = a_0 + a_1X_1 + a_2X_2$ is a plane; $V = b_0 + b_1X_1 + b_2X_2 + b_{12}X_1X_2 + b_{11}X_1^2 + b_{22}X_2^2$ is a parabolic. The E-plane over the efficient portfolio set is a series of connected line segments. The section of the V-parabolic over the efficient portfolio set is a series of connected parabola segments. It plotted V against E for efficient portfolios it would again get a series of connected parabola segments. This result obtains for any number of securities. Various reasons recommend the use of the expected return-variance of return rule, both as a hypothesis to explain well-established sender behavior and as a maximum to guide. The rule serves better, as an explanation of, and guide to, "investment" as distinguished from ("speculative" behavior. 10. Just as we used the equation $5X_i = I$ to reduce the dimensionality in the three $i=1$ security case, we can use it to represent the four security case in 3 dimensional space. Eliminating X , we get $E = E(X_1, X_2, X_3)$, $V = V(X_1, X_2, X_3)$. The attainable set is represented, in three-space, by the tetrahedron with vertices (0,0,0), (0,0,1), (0,1,0), (1,0,0), representing portfolios with, respectively, $X_4 = 1$, $X_3 = 1$, $X_2 = 1$, $X_1 = 1$. As in the two dimensional case the point with minimum available variance may be in the interior of the available set or on one of its boundaries. Typically this proceeds along a given critical line until either this line intersects one of a larger subspace or meets a boundary (and simultaneously the critical line of a lower dimensional subspace). In either of these cases the efficient line turns and continues along the new line. The efficient line terminates when a point with maximum E is reached.

VII. PERFORMANCE ANALYSIS

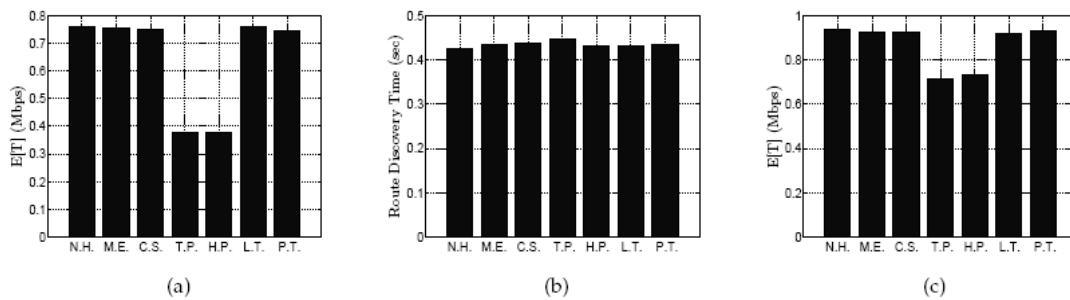
In order to quantify the impact of selective jamming, this system measures the application delay until the file transfer was completed. It also measured the average effective throughput of the TCP connection as the fraction of the file size over the time until the file transfer was completed. Finally, this system measured the number of packets that the adversary blocked in each of the four jamming strategies. In Figure (a), it shows the application delay as a function of the jamming probability p . In Figure (b), it shows the average effective throughput of the TCP connection as a function of p . Finally, Figure (c) depicts the number of packets that were jammed by the adversary for each value of p . It observes that for a TCP connection, a selective jamming attack against TCP ACKs is significantly more harmful and efficient than all other jamming strategies. By jamming 40% of TCP ACKs, the application delay is one order of magnitude larger compared to jamming just data, and two orders of magnitude larger than jamming RTS or CTS messages at the MAC layer. Moreover, for values of p larger than 0.4, the TCP connection was aborted due to the repeated timeout of the sender. Likewise, the average effective throughput drops significantly faster when TCP ACKs are jammed, compared to jamming regular data transmissions or RTS and CTS message exchanges as it is shown in Figure (b). The interpretation of the effectiveness of the selective jamming of TCP ACKs lies in the congestion control mechanism of the TCP protocol. When cumulative ACKs are lost or also called as jamming, the sender has to retransmit all

unacknowledged data packets, thus increasing the incurred delay while reducing the effective throughput. At the same time, the sender interprets the loss of ACKs as congestion and throttles its packet transmission rate by reducing the size of the transmission window. This leads to a further slowdown of the application. A critical observation in Figure (c) is that as the packet transmission rate of the sender drops, the jammer has to jam fewer TCP ACKs thus reducing the amount of time that the jammer has to remain active. Then the MAC layer, the number of transmission attempts for data packets is four. Hence, in order to successfully jam a TCP ACK, a total of four messages need to be jammed. On the other hand RTS/CTS messages are retransmitted a total of seven times before the sender stops its retransmission attempts. It is therefore much harder to drop all RTS/CTS retransmissions relevant to a data packet that would cause its retransmission at the TCP layer. In addition, RTS/CTS packets are significantly smaller (20 bytes long) compared to data packets, making their retransmission fairly fast. Thus, selective jamming against ACKs or data is more effective than targeting control packets at the MAC layer. To overcome such jamming a portfolio theory are implemented for the efficient data transmission.



VIII. EVALUATION OF PACKET-HIDING TECHNIQUES

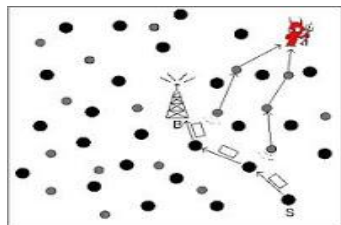
The impact of the packet-hiding techniques on the network performance is controlled via extensive simulations. OPNET Modeler is the software used for network simulation purpose and it has different version of modeler in which modeler 14.5, are used in packet hiding techniques. In general, OPNET Modeler comprises a suite of protocols and technologies, and features a sophisticated development environment. By modeling all network types and technologies (including VoIP, TCP, OSPFv3, MPLS, IPv6 and more), OPNET Modeler helps to analyses realistic simulated networks to compare the impact of different technology designs on end-to-end behavior. OPNET Modeler is used to test and demonstrate technology designs in realistic scenarios before production. OPNET MODELER 14.5 is to implement the hiding sub layer and measure its impact on the effective throughput of end-to-end connections and on the route discovery process in wireless ad-hoc networks. A set of nodes running 802.11b, it is a network standard at the PHY and MAC layers, AODV is a routing protocol for route discovery, and TCP at the transport layer. Aside from this method, it also implemented a simple MAC layer encryption with a static key. This is due to the cryptographic puzzle that must be solved at the receiver. The processing delay of the various schemes is taken into account in the experimental evaluations. In the first set of experiment, the setup is a single file transfer between a client and server, connected via a multi-hop route. The client requested a 1 MB file from the server. The effects of packet hiding by measuring the effective throughput of the TCP connection in the following scenarios: (a) No packet hiding (N.H.), (b) MAC-layer encryption with a static key (M.E.), (c) SHCS (C.S.), (d) Time-lock CPHS (T.P.), (e) Hash-based CPHS (H.P.), (f) Linear AONT-HS (L.T.), and (g) AONT-HS based on the package transform (P.T.).



(a) Average effective throughput (line network topology), (b) average route discovery time (non-congested network), (c) average effective throughput (congested network). N.H.: No packet hiding, M.E.: MAC-layer encryption with a static key, C.S.: SHCS, T.P.: Time-lock CPHS, H.P.: Hash-based CPHS, L.T.: Linear AONT-HS, P.T.: Package transform.

IX. NON-SELECTIVE JAMMING ATTACKS

Conventional methods for mitigating jamming employ some form of Spread Spectrum (SS) communications. The transmitted signal is spread to a larger bandwidth following a Pseudo-noise (PN) sequence. Without the knowledge of this sequence, a large amount of energy is required to interfere with an ongoing transmission. However, in the case of broadcast communications, compromise of commonly shared PN codes neutralize the advantages of SS. In the proposed system a jamming-resistant communication model for pair wise communications that does not rely on shared secrets. Communicating nodes use a physical layer modulation



method called Uncoordinated Direct- Sequence Spread Spectrum (UDSSS). Uncoordinated direct sequence spread spectrum (UDSSS) is a spread spectrum communication scheme where the sender and the receiver communicate using secret spreading codes that they choose randomly and independently from a public set of channels. The receiver is unaware of the codes used by the sender to transmit the messages prior to their communication. They also proposed a jamming-resistant broadcast method in which transmissions are spread according to PN codes randomly selected from a public codebook. Several

other schemes eliminate overall the need for secret PN codes.

X. EXPERIMENTAL ANALYSIS

In the experiments, the impact of packet hiding on the route discovery process in an ad-hoc network. It generates a random topology of 54 nodes placed in an area of 500×400 m². Nodes discover routes using the AODV routing protocol. A total of twenty client/server pairs exchange messages of size 1 KB using the TCP protocol, at randomly chosen starting times. The size of the message exchanged between pairs of nodes was kept small in order to avoid skewing of the route discovery performance due to network congestion. This delay is defined as the time difference between the transmission of the first Route-Request (RREQ) from a source and the reception of the corresponding Route-Reply (RREP) from the destination. The impact of packet hiding on the route discovery delay is minimal compared to the case where no packet hiding is employed. This similarity in performance is due to the expanding ring search technique of Ad hoc On-Demand Distance Vector (AODV), which is used to prevent unnecessary network wide dissemination of RREQs. In order to discover a route, the originating node sends a RREQ with a time to-live (TTL) value equal to one hop, and waits for the corresponding RREP. If the RREP is not received before the timeout value expires, the originating node increases the TTL and the timeout to, and re-broadcasts the RREQ. This process is repeated until a valid RREP is received, or the TTL value exceeds the maximum diameter of the network. The expanding ring search technique introduces a dominant delay, in comparison to the delay introduced by the packet-hiding techniques.

XI. CONCLUSION

The selective jamming attacks usually occur in the network between sources to destination nodes the cryptographic methods of packet transaction are accomplished but the drawback in it are, Where the hacker or the third party can easily recognize the message and they can easily decrypt the cipher text where by this method of decrypting the cipher text, the third party are usually hidden and their attacks are unknown to the sender and receiver such attack are generally called as duplicate jamming which is to identify the route, which is jammed because of hacker or third party. The portfolio theory are implemented and it easily identifies the route in which jamming are occurred and they just eliminate that particular route and transform the packet in the route where there is no jamming taken place by this way the efficient packet transaction are taken place between the sender and the receiver. Dynamic Source Routing (DSR) or Ad Hoc On-Demand Distance Vector (AODV) is the routing algorithms are used in the packet transmission. Portfolio selection theory is used to calculate the best route by calculating the threshold value. The threshold value is calculated on the route based the path cost and by building the path table.

REFERENCES

- [1] 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.
- [2] 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.
- [3] A.Chan, X. Liu, G. Noubir, and B. Thapa. "Control channel jamming: Resilience and identification of traitors". In Proceedings of ISIT, 2007.
- [4] 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.
- [5] Y. Desmedt. "Broadcast anti-jamming systems". Computer Networks, 35(2-3):223–236, February 2001.
- [6] K. Gaj and P. Chodowicz. "FPGA and ASIC implementations of AES". Cryptographic Engineering, pages 235–294, 2009.
- [7] O. Goldreich. "Foundations of cryptography": Basic applications. Cambridge University Press, 2004.
- [8] B. Greenstein, D. McCoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. "Improving wireless privacy with an identifier-free link layer protocol". In Proceedings of MobiSys, 2008.
- [9] IEEE. IEEE 802.11 standard. <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>, 2007.
- [10] A.Juels and J. Brainard. "Client puzzles: A cryptographic countermeasure against connection depletion attacks". In Proceedings of NDSS, pages 151–165, 1999.