IPHV7I20039X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

SECURE ANTI JAMMING SYSTEM FOR WIRELESS SENSOR NETWORKS MAC PROTOCOLS

[#1] Sheik Jakeer,[#2] M.Naresh
Department of Computer Science & Engineering,
Newton's Institute Of Engineering, Macherla.

Abstract: - The problem of efficiently and securely broadcasting to a remote cooperative group occurs in many newly emerging networks. Jamming attacks are much harder to counter and more security problems. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. This intentional interference with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. 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. In this work, we address 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. We illustrate 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. We show those selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. We analyze the security of our methods and evaluate their computational and communication overhead.

Keywords:- *Wireless Network, Broadcast, Network Scalability, Denial-of-Service, Selective Jamming.*

I.INTRODUCTION

WMNs have been recently suggested as a promising low-cost approach to provide last-mile high-speed Internet access. A typical WMN is a multihop hierarchical wireless network. The top layer consists of high-speed wired Internet entry points. The second layer is made up of stationary mesh routers serving as a multihop backbone to connect to each other and Internet via long-range high-speed wireless techniques. The bottomlayer includes a large number of mobile network users. The end-users access the network either by a direct wireless link or through a chain of other peer users leading to a nearby mesh router; the router further connects to remote users through the wireless backbone and Internet. Security and privacy issues are of utmost concern in pushing the success of WMNs for their wide deployment and for supporting service-oriented applications. For instance, a manager on his way to holiday may want to send a confidential e-mail to some staff of her company viaWMNs, so that the intended staff members can read the e-mail with their mobile devices (laptops, PDAs, smartphones, etc.). Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce access control of sensitive information to cope with both eavesdroppers and malicious attackers. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. hey have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses [17]. Typically, jamming attacks have been considered under an external threat

model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of highpower interference signals. However, adopting an "always-on" strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect. Conventional anti-jamming techniques rely extensively on spread-spectrum (SS) communications, or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats [37]). SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model. Potential disclosure of secrets due to node compromise, neutralizes the gains of SS. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information. In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching *selective jamming attacks* in which specific messages of "high importance" are targeted. 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 adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly. 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 adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver [34]. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

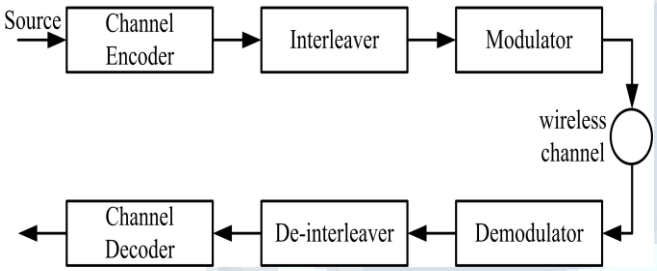
II. RELATED WORK

WMNs have been recently suggested as a promising low-cost approach to provide last-mile high-speed Internet access. A typical WMN is a multihop hierarchical wireless network. The top layer consists of high-speed wired Internet entry points. The second layer is made up of stationary mesh routers serving as a multihop backbone to connect to each other and Internet via long-range high-speed wireless techniques. The bottomlayer includes a large number of mobile network users. The end-users access the network either by a direct wireless link or through a chain of other peer users leading to a nearby mesh router; the router further connects to remote users through the wireless backbone and Internet. Security and privacy issues are of utmost concern in pushing the success of WMNs for their wide deployment and for supporting service-oriented applications. For instance, a manager on his way to holiday may want to send a confidential e-mail to some staff of her company viaWMNs, so that the intended staff members can read the e-mail with their mobile devices (laptops, PDAs, smartphones, etc.). Due to the intrinsically open and distributed nature of WMNs, it is essential to enforce access control of sensitive information to cope with both eavesdroppers and malicious attackers. A MANET is a system made up of wireless mobile nodes. These nodes have wireless communication and networking characteristics. MANETs have been proposed to serve as an effective networking system facilitating data exchange between mobile devices even without fixed infrastructures. In MANETs, it is important to support group-oriented applications, such as audio/video conference and one-to-many data dissemination in battlefield or disaster rescue scenarios. In general, users working for the same mission form a cooperation domain; any particular application or interest in a network may lead to the establishment

IPHV7I20039X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

of a corresponding community. Since communication in wireless networks is broadcast and a certain amount of devices can receive transmitted messages, the risk of unsecured sensitive information being intercepted by unintended recipients is a real concern. For instance, a commander may issue secret commands to soldiers in battlefield via satellite-to-MANET communication. Consequently, efforts to secure group communications in MANETs are essential.

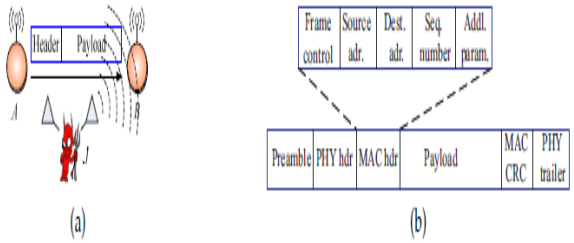
PROPOSED METHOD:



In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. 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 adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly. 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 adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver [34]. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

III.IMPLEMENTATION

We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. 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.



(a) Realization of a selective jamming attack, (b) a generic frame format for a wireless network.

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 preshared pairwise keys or asymmetric cryptography.

Selective Jamming:

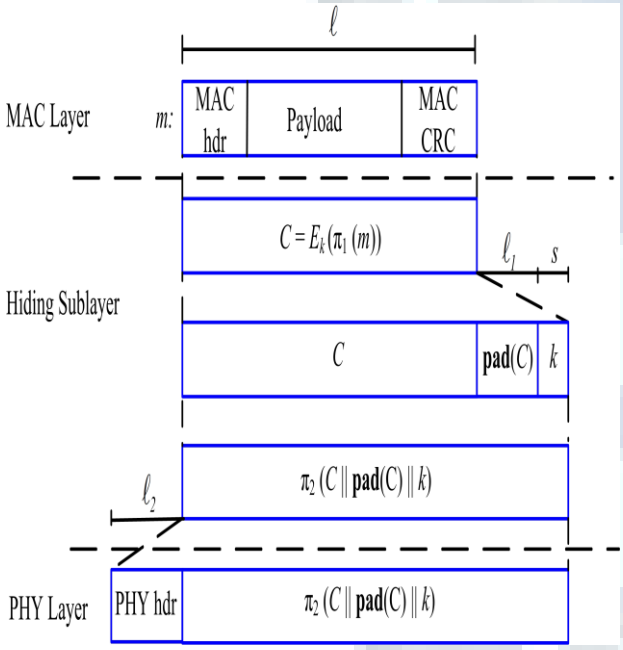
We illustrate the impact of selective jamming attacks on the network performance. implement selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. An adversary in possession of the decryption key can start

IPHV7I20039X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

decrypting as early as the reception of the first ciphertext block.

IV. Strong Hiding Commitment Scheme (SHCS)

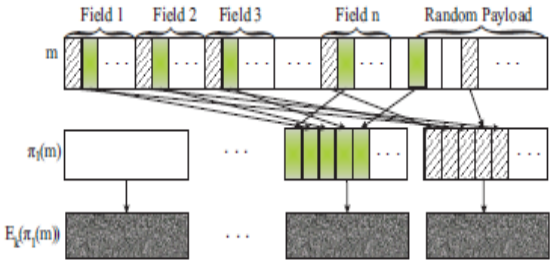
We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum.



The computation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined. However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed . If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thus\ avoiding the decryption operation at the receiver.

V. Cryptographic Puzzle Hiding Scheme (CPHS)

We present a packet hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he 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.



Application of permutation π_1 on packet m.

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 We consider several puzzle schemes as the basis for CPHS. For each scheme, we analyze the implementation details which impact security and performance. Cryptographic puzzles are primitives originally suggested by Merkle as a method for establishing a secret over an insecure channel. They find a wide range of applications from preventing DoS attacks to providing broadcast authentication and key escrow schemes.

VI. ENHANCED PACKET DELIVERY TECHNIQUES

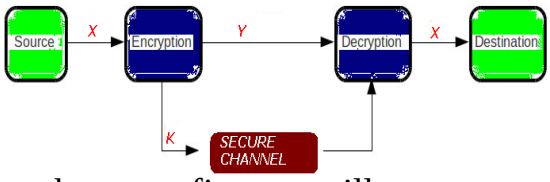
In this section, we show that the problem of real-time packet classification can be mapped to the hiding property of binder schemes, and propose a packet-hiding scheme based on binder. In our context, the role of the committer is assumed by the transmitting node S. The role of the verifier is assumed by any receiver R, including the jammer J. The committed value m is the packet that S

IPHV7I20039X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

wants to communicate to R. To transmit m, the sender computes the corresponding binder/de-binder pair (C, d), and broadcasts C. The hiding property ensures that m is not revealed during the transmission of C. To reveal m, the sender releases the de-commitment value d, in which case m is obtained by all receivers, including J. Here We explain in detail about packet delivery Techniques.

Secrete Technique

Here we explain a method Secrete Technique which includes the symmetric cryptography._ Encryption is the security solution most applicable in computing. In recent years asymmetric Algorithms have been extensively studied in embedded systems with low computational power._Data encryption emerged before the invention of_ computer. a cryptographic algorithm can be set as a function that converts encrypted message in clear messages and vice versa, making use of a cryptographic key. Most cryptographic algorithms are public. Secrecy is the key that has the function to parameterize the cryptographic function; i.e only with the key can encrypt or decrypt a message. Another important factor is that the key have the ability to change the output of the algorithm, so every change of key cryptographic algorithm generates a new encrypted message. The key size is critical in a project, because the longer the key, more work will be crypto analyst to try to decipher the message. In general, keys have sizes of 64, 128 or 256 bits and may be higher or lower, according to security needs. Symmetric encryption or secret key cryptography is the use of only a key, both in the encryption and decryption of data. By the year 1976 this was the only known method for the use of encryption, but to be effective you need a secure channel for communication in which a cryptographic key can be changed.



The above figure illustrates a communication through symmetric encryption. The text is encrypted X and Y become the message through the encryption algorithm and key k. The message Y is sent to the receiver, which uses the key k to decrypt it, turning it on again in the text X. Also according to figure 6 you can see that the key k is transported by a secure channel, for the possession of it, a potential attacker could easily make the reading the original text. AES and DES are two examples of algorithms that are part of the class symmetrical.

Our Main Aim is to satisfy the heavy secrecy on hiding property. Assume sender S has send the Packet m for R then sender construct the Secrete Technique, its includes the any Encryption Algorithm. Like AES,DES..etc .

(C, d) = commit(m), where,

C = Ek(∧1(m)), d = k.

Here, the function Ek() is a symmetric encryption algorithm ∧1 is a publicly known permutation, and k ϰ {0, 1}s is a randomly selected key of some desired key length s (the length of k is a security parameter). The sender broadcasts (C||d), where "||" denotes the concatenation operation. Upon reception of d, any receiver R computes m = ∧**í1** (Dk(C)) where ∧í1 denotes the inverse permutation

IPHV7I20039X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

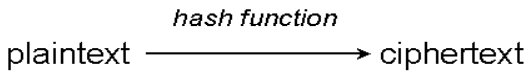
of ∧1. To satisfy the hiding property, the packet carrying d is formatted so that all bits of d are modulated in the last few PHY layer symbols of the packet. To recover d, any receiver must receive and decode the last symbols of the transmitted packet, thus preventing early disclosure of d.

Cryptologic Riddle

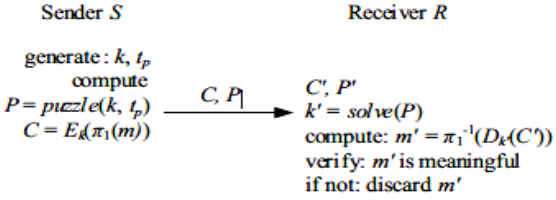
In this section, we present a packet beating system based on Cryptologic Riddle. The main idea behind such riddles is to force the recipient of a riddle execute a pre-defined set of calculations before he is able to extract a secret of interest. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. There are several ways of classifying cryptographic algorithms. They will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The three types of algorithms that will be discussed

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

Here the technique Croptologic Riddle based on hashing.



Computationally limited receivers can incur significant delay and energy consumption when dealing with modulo arithmetic. In this case, Cryptologic Riddle can be implemented from cryptographic puzzles which employ computationally efficient cryptographic primitives. Cryptologic Riddle are primitives originally suggested by Merkle as a method for establishing a secret over an insecure channel. They find a wide range of applications from preventing DoS attacks to providing broadcast authentication and key escrow schemes.



In our context, we use cryptographic puzzles to temporary 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. Let a sender S have a packet m for transmission. The sender selects a random key k א {0, 1}s, of a desired length. S generates a puzzle P = puzzle(k, tp), where puzzle() denotes the puzzle generator function, and tp denotes the time required for the solution of the puzzle. Parameter tp is measured in units of time, and it is directly dependent on the assumed computational capability of the adversary, denoted by N and measured in computational operations per second.

After generating the puzzle P, the sender broadcasts (C, P), where C = Ek(∧1(m)). At the receiver side, any receiver R solves the received puzzle Pϱ to recover key kϱ and then computes mϱ = ∧í1(Dkϱ (Cϱ)). If the decrypted packet mϱ is meaningful (i.e., is in the proper format, has a valid CRC code, and is within the context of the receiver's communication), the receiver accepts that mϱ = m. Else, the receiver discards mϱ. Fig. 8 shows the details of Cryptologic Riddle.

Her we discuss about various types of Riddles, which are worked based on the crypotologic.

Time-Lock Riddle

Simple Substitution Cipher Riddle Transposition Ciphers Riddle Book Cipher Riddle Poly-Alphabetic Cipher Riddle. Poly-Graphic Cipher Riddle

VI.CONCLUSION

We addressed the problem of selective jamming attacks in wireless networks. We considered an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. We showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. We evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective jammer can significantly impact performance with very low effort. We developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Our schemes combine cryptographic primitives such as 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.

REFERENCES

[1] Packet-Hiding Methods for Preventing Selective Jamming Attacks, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING ,VOL. 9, NO. 1, JAN-FEB 2012
[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. Chodowiec. 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.IEEE802.11standard. 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.
[11] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. ACMTransactions on Sensors Networks, 5(1):1–38, 2009.
[12] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pages 169–180, 2009.
[13] G. Lin and G. Noubir. On link layer denial of service in data wireless LANs. Wireless Communications and Mobile Computing, 5(3):273–284, May 2004.
[14] X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers using multi-layer agility. In Proceedings of INFOCOM, pages 2536– 2540, 2007.
[15] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In Proceedings of INFOCOM, San Diego, 2010.
[16] R. C. Merkle. Secure communications over insecure channels. Com- munications of the ACM, 21(4):294–299, 1978.
[17] G. Noubir and G. Lin. Low-power DoS attacks in data wireless lans and countermeasures. Mobile Computing and Communications Review, 7(3):29–30, 2003.

AUTHORS PROFILE:

[1] Sheik Jakeer Pursuing M.Tech in CSE at Newton's Institute of Engineering,Macherla.

[2] M.NARESH, M.Tech working as Associate Professor, department of CSE at Newton's Institute Of Engineering, Macherla.