RESEARCH ARTICLE OPEN ACCESS

Preventing Real-Time Packet Classification Using Cryptographic Primitives

N.Vasumathi[1], P.Ramadoss[2], V.Nancy[3]
[1]M.E. Computer Science and Engineering Parisutham Institute of Technology & Science Affiliated to Anna University Chennai Tamil Nadu- India
[2]Assistant Professor Parisutham Institute of Technology and Science Affiliated to Anna University Chennai Tamil Nadu- India
[3]M.E. Computer Science and Engineering Parisutham Institute of Technology & Science Affiliated to Anna University Chennai Tamil Nadu- India

Abstract
Jamming attacks are especially harmful when ensuring the dependability of wireless communication. Typically, jamming has been addressed under an external threat model. 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 addressed in this work. In these attacks, the adversary is active only for a short period of time, specifically targeting messages of high importance. The advantages of selective jamming in terms of network performance degradation and adversary effort is illustrated by presenting two case studies; one is selective attack on TCP and another is on routing. The selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To avoid these attacks, four schemes are developed such as All Or Nothing Transformation-Hiding Scheme (AONT-HS) - pseudo message is added with message before transformation and encryption, Strong Hiding Commitment Scheme(SHCS) - off-the-shelf symmetric encryption is done, Puzzle Based Hiding Scheme(PBHS)- time lock and hash puzzle and Nonce based Authenticated Encryption Scheme(N-AES)-Nonce is used for encryption, that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes.
Index Terms— Selective jamming, Pseudo message, Symmetric encryption, Time lock puzzles, Nonce based Authentication.

I. Introduction

Wireless Local Area Networks (WLANs) are becoming an increasingly important technology that is bringing the world closer together. WLANs are essential in every area, such as education, agriculture, manufacturing, transportation, military, research and so on. Therefore, the WLAN security is very significant. There are two popular styles of WLANs: Client-server networks and Ad-hoc networks. The variation between these two networks is that client-server networks use access points or routers to transmit data, but ad-hoc networks do not rely upon any pre-existing transmitters. Alternatively, all the nodes in an ad-hoc network participate in the routing process by forwarding messages to each other.

All wireless network nodes transmit data packets in different channels. Hence channels in WLANs are defined by frequencies; they are susceptible to malicious jamming attacks which is easy for attackers to accomplish sending multitudes of useless packets in a specific frequency. Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. Anyway, the open nature of this medium leaves it vulnerable to multiple security threats. Any nodes with a transceiver can eavesdrop on wireless transmissions, add spurious messages, or jam legitimate ones. While message injection and eavesdropping can be prevented using cryptographic methods, jamming attacks are very difficult to counter. They have been identified to actualize severe Denial-of-Service (DoS) attacks against wireless networks. The adversary interferes with the reception of messages by transmitting a continuous jamming signal or several short jamming pulses.

Typically, jamming attacks have been considered under an external threat model, where jammer is not part of the network. Under this model, jamming techniques include the continuous or random transmission of high-power interference signals. However, adopting an "always-on" strategy has several drawbacks. First, the adversary has to expend a vast amount of energy to jam signals of interest. Second, the continuous transmission 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)SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. Hence these methods can only protect wireless transmissions under the external threat model.

Potential disclosure of secrets due to node compromise neutralizes the gains of Spread Spectrum. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Thus, the compromise of a single receiver is enough to reveal relevant cryptographic information. To launch selective jamming attacks, the adversary must have capability to implement a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be done either by classifying transmitted packets using protocol semantics or by decoding packets during transmission. In the next method, the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as type of the packet, source and destination address. After classifying those data, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. Selective jamming requires knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

1.1Wireless LAN Security

Wireless LAN security has come a long way since the early days and the negative publicity around the shortcomings of WEP. Recent advances in WLAN technology and the ratification of key wireless security standards are giving Network administrators the high level of confidence in WLAN security that they have always needed. To be effective, WLAN security must address three critical areas;

- Data Confidentiality and Integrity,
- Authentication and Access Control
- Intrusion Detection and Prevention

1.2WLAN Security Threats

The nature of networking means that users can exchange information across a distance and over a shared medium. The security breach of this is that a hacker does not need to actually walk up to a server or a user's computer in order to gain access to critical files or communications. In W LAN, this threat is especially mentioned, because a hacker doesn't need to reside in the same physical location. Some Threats to the wireless network initially stem from providing openings like those described below

1.2.1Unauthorized Client Access

Hackers continually probe areas for open wireless networks. If a network has a weak user authentication scheme – or none at all – it is very easy for a hacker to obtain access to the corporate network and take information or launch attacks on resources in order to cause disruptions.

1.2.2Denial of Service (DoS)

Because of the way networking devices work, they need to respond to any client requests. Hackers are able to exploit this by inundating a network resource with more requests than it is able to handle. Distributed DoS attacks magnify this problem by enlisting a number of unknowing computers through hidden code to simultaneously launch denial of service attacks on a potentially massive scale.

1.2.3Man in the Middle

If data is unsecured, hackers can intercept messages and change the content to mislead parties that are communicating, making it seem as if the hacker is actually one of the parties.

1.2.4 IP Spoofing

By modifying the source IP address contained in the packet header, a hacker can intercept traffic coming from a legitimately authenticated user and make it appear that the user is actually using the hacker's computer. As a result, all data and messages coming from a server would go back to the hacker.

II. Existing Work

2.1Existing concepts & methodology

Conventional anti-jamming techniques rely extensively on Spread-Spectrum (SS) communications or some form of jamming evasion (e.g., slow frequency hopping). SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating nodes. These methods can only protect wireless transmissions under the external threat model.

2.2 Problem statement

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, add spurious messages, or jam legitimate ones. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.

III. Proposed Work

3.1objective

To show that selective jamming attacks can be launched by performing real time packet classification at the physical layer. To reduce these attacks schemes are developed that prevent real-time packet classification by combining cryptographic primitives with physical layer attributes. An intuitive solution to selective jamming would be the encryption of transmitted packets (including headers) with a key. For broadcast communications, this static key must be known to intended receivers and hence, is vulnerable to compromise. Even if the encryption key of a hiding scheme were to kept secret, the static parts of a transmitted packet could potentially lead to packet classification. To avoid these attacks, four schemes are developed such as All Or Nothing Transformation-Hiding Scheme (AONT-HS) - pseudo message is added with message before transformation and encryption, Strong Hiding Commitment Scheme(SHCS) - off-the-shelf symmetric encryption is done, Puzzle Based Hiding Scheme(PBHS)- time lock and hash puzzle and Nonce based Authenticated Encryption Scheme(N-AES)-Nonce is used for encryption, that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes.

3.2All or Nothing Transformation Hiding Scheme

AONT-HS represents All or Nothing Transformation Hiding Scheme. 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. A transformation f, mapping message m = {m1, · · ·, mx} to a sequence of pseudo-messages m′ = {m′ 1 , · · · , m′ x′} In this context, packets are pre-processed by an AONT before transmission but left unencrypted. Thus, the jammer cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. Packet m is split to a set of x input blocks m = {m1. . . mx}, which serve as an input to an AONT f : {Fu} x → {Fu} x ′ . Here, Fu denotes the alphabet of blocks mi and x ′ denotes the number of output pseudo-messages with x ′ ≥ x.

The set of pseudo-messages m′ = {m′ 1 . . . m′ x′} is transmitted over the shared wireless medium. At the receiver end, the inverse transformation f −1 is applied after all x ′ pseudo-messages are received, in order to obtain m.

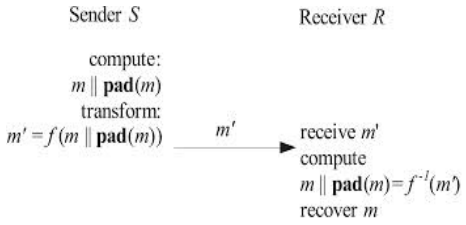

Fig 1: All Or Nothing Transformation Hiding Scheme

3.3Puzzle based Hiding Scheme

The basic 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 needed for obtaining the solution of a puzzle depends on its hardness and the computational ability of the puzzle solver. The advantage of the puzzle based hiding scheme is that its security does not rely on the PHY layer parameters. It has higher computation and communication overhead. Here puzzles are used to temporarily hide transmitted packets. A packet m is enciphered with a randomly selected symmetric key (k) of a desirable length s. The key k is blinded using a puzzle and sent to the receiver. For a computationally bounded receiver or adversary, the puzzle carrying k is difficult to be solved before the transmission of the encrypted version of m is completed and the puzzle is received. Thus, the adversary cannot classify the packet m for the purpose of selective jamming.

3.3.1Time-lock Puzzle

It is based on the iterative application of a precisely controlled number of modulo operations. Time-lock puzzles have more attractive features such as the fine granularity in controlling tp and the sequential nature of the computation. Also, the puzzle generation requires significantly less computation compared puzzling. In this type of puzzle, the puzzle constructor generates a composite modulus g = u ・ v, where u and v are two large random prime numbers. Then, he picks a random a, 1 < a < g and hides the encryption key in Kh = k + a2t mod g, where t = tp ・ N, is the amount of time required to solve for k. Here, it is considered that the solver can perform N squarings mod(g) per second. Note that Kh can be calculated efficiently if φ(g) = (u − 1)(v − 1) or the factorization of g are known, otherwise a solver would have to do all t squarings to recover k. The puzzle consists of the values P = (g,Kh, t, a).

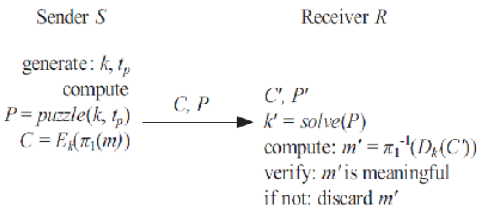

Fig 2: Puzzle based Hiding Scheme

3.3.2Puzzles based on hashing

Computationally limited receivers can incur significant delay and energy consumption when dealing with modulo arithmetic. Here, CPHS can be implemented from cryptographic puzzles which employ computationally efficient cryptographic primitives. Client puzzles, use one-way hash functions with partially disclosed inputs to force puzzle solvers search through a space of a precisely controlled size. In this context, the sender picks a random key k with k = k1||k2. The lengths of k1 and k2 are s1, and s2, respectively. Then he computes C = Ek(π1(m)) and transmits (C, k1, h(k)) by this particular order. To recover k, any receiver has to perform on average 2s2−1 hash operations (assuming perfect hash functions). Since the puzzle cannot be solved before h(k) has been received, the receiver or any adversary cannot classify m before the completion of m's transmission.

3.4Strong Hiding Commitment Scheme

SHCS represents Strong Hiding Commitment Scheme. The main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum. Consider that the sender S has a packet m for R. First, S constructs (C, d) = commit (m), where, C = Ek(π1(m)), d = k. Here, the commitment function Ek() is an off-the-shelf symmetric encryption algorithm (e.g., Triple DES), π1 is a publicly known permutation, and k ∈ {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. On reception of d, any receiver R computes m = π¯1(Dk(C)), where π −1 1 denotes the inverse permutation of π1. To achieve the strong hiding property, the packet containing d is formatted so that all bits of d, are harmonized in the last few PHY layer attributes of the packet. To obtain d, any receiver must receive and decode the last symbols of the transmitted packet, hence avoiding early disclosure of d.

3.4.1Permutation

This scheme applies two publicly known permutations π_1 and π_2 at different processing stages. Permutation π_1 is applied to m before it is encrypted. The purpose of π_1 is twofold. Initially, it distributes critical frame fields which can be used for packet classification across multiple plaintext blocks. Thus, to reconstruct these fields, all corresponding cipher blocks must be received and deciphered. Also, header information is pushed at the end of π_1 (m). This prevents early reception of the corresponding ciphertext blocks.

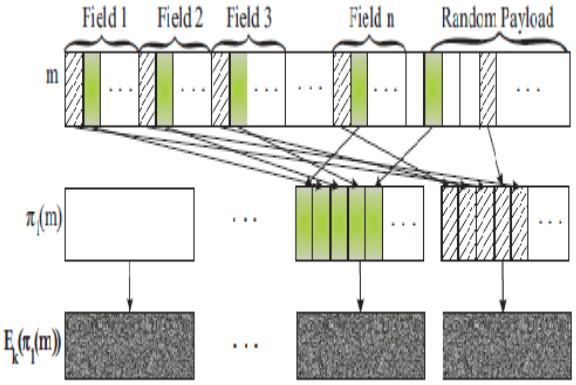

Fig 3: Application of permutation π1 on packet m.

3.5Nonce based Authenticated Encryption Scheme

MAC tree construction is used to build a file encryption scheme. Let D = D_1.....D_n where D_i ε $\{0,1\}^d$ the content of the file. Nonce-based authenticated encryption scheme is applied to each file block D_i, using the leafcounter $N_i^{(0)}$:(C_i, T_i) ← $E_K(N_i^{(0)}, D_i)$,and store the ciphertextC_i and the authentication tag T_i to the untrusted storage, along with the MAC tree for maintaining the leaf counters $N_i^{(0)}$. A simple authenticated encryption scheme is constructed as composition of the CTR encryption mode of operation and the MAC scheme. Figure shows the composite scheme: using the counter $N_i^{(0)}$, a pseudorandom sequence is generated by the Counter mode, the file block D_i is XORed with this sequence to produce the ciphertext block C_i, and the counter $N_i^{(0)}$ is used to authenticate C_i, producing the authentication tag T_i.Special care is needed to never re-use a nonce throughout our construction. Note that here the counter $N_i^{(0)}$ is used both for encryption and authentication. In fact, here the counter is not used directly, but uses different encoding schemes to generate non-repeating nonces.

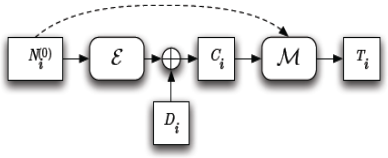

Fig 4: Block-wise Authenticated based Encryption

3.5.1Security of the scheme

Intuitively, it is easy to see that, if MAC tree construction is not used, and instead manage all of the leaf counters $N_k^{(0)}$ in the trusted storage, then this scheme guarantees both confidentiality and integrity of the file content: all the block counters $N_k^{(0)}$ are properly incremented, and no nonce is repeated, and each file blocks are encrypted and authenticated independent from each other. Essentially, the confidentiality and the integrity of the resulting scheme come from the security of the composite authenticated encryption scheme, and the nonce-respecting property. In this scheme, instead of managing the leaf counters in the trusted storage, they are stored in MAC tree and store only the root counter in the trusted storage. Still, from the way the MAC tree is constructed, the trust of the root counter can be transferred to its descendants, as long as all of the tag verifications along the path are successful. In this way, it is ensured that our MAC tree construction can safely replace counters stored in a trusted storage, except negligible probability of successful attack.

IV. System Design

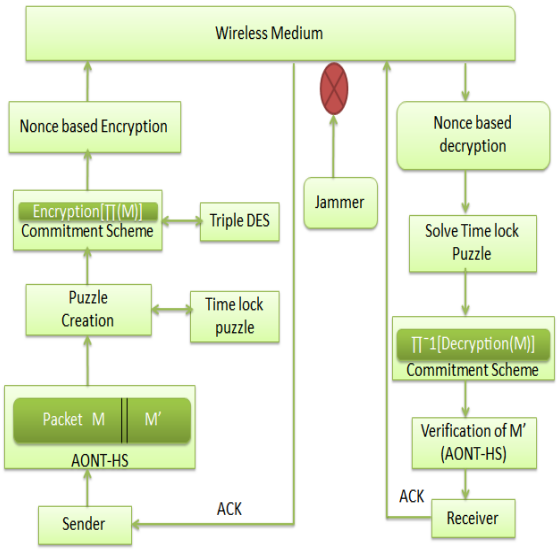

Fig 5: Architecture for preventing real time packet classification

V. Conclusion

The problem of selective jamming attacks in wireless networks is addressed in this work. In these attacks, the adversary is active only for certain period of time, specifically targeting messages of high importance. The advantages of selective jamming in terms of network performance degradation and adversary effort is illustrated. An internal adversary model is considered, where the jammer is one of the parts of the network under attack, thus it is aware of the protocol specifications and shared network secrets. The selective jammer can significantly impact performance with very low effort. The selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To avoid these attacks, four schemes are developed such as All Or Nothing Transformation-Hiding Scheme (AONT-HS) - pseudo message is added with message before transformation and encryption, Strong Hiding Commitment Scheme(SHCS) - off-the-shelf symmetric encryption is done, Puzzle Based Hiding Scheme(PBHS)- using time lock and hash puzzles and Nonce based Authenticated Encryption Scheme(N-AES)-Nonce is used for encryption, that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes.

VI. Future Work

To improve the efficiency of these schemes in terms of time by using cryptography based algorithms which consumes less time and provides more security.

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 anti-jamming 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, P. Chodowiec, FPGA and ASIC implementations of AES."Cryptographic Engineering",pages 235–294, 2009.

[7] R. Rivest. "All-or-nothing encryption and the package transform". Lecture Notes in Computer Science, pages 210–218, 1997.

[8] R. Rivest, A. Shamir, and D. Wagner. "Time-lock puzzles and timed release crypto". Massachusetts Institute of Technology, 1996

[9] B. Schneier."Appliedcryptography: protocols, algorithms, and source code in C".John Wiley & Sons, 2007.