Combining Elliptic Curve Cryptography to Prevent Attacks for Secure Network Route Discovery

A. MADHURI[1] ,S. RAJIYA SULTANA[2]

[1]MTech Student of Bharath College of Engineering and Technology for Women, Kadapa, AP, India

[2]MTech, Assistant Professor of Bharath College of Engineering and Technology for Women, Kadapa, AP, India

ABSTRACT: Wireless networks have many applications, vary in size, and are deployed in a wide variety of areas. As the wireless industry explodes, it faces a growing need for security.

Both for secure (authenticated, private) Web transactions and for secure (signed, encrypted) messaging, a full and efficient Public Key Infrastructure is needed.They are often deployed in potentially adverse or even hostile environment so that there are concerns on security issues in these networks. The Open Nature of wireless medium leaves an intentional interference attack, typically referred to as jamming.To mitigate these attacks, we develop three schemes that prevent real time packet classification by combining cryptographic primitives with physical-layer attributes. They are Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), All-Or-Nothing Transformation Hiding Schemes (AONTSHS). Random key distribution methods are done along with three schemes to give more secured packet transmission in wireless networks. Additionally,we combine elliptic curve cryptography to prevent attacks.

Efficient key distribution and management mechanisms are needed besides lightweight ciphers. Many key establishment techniques have been designed to address the tradeoff between limited memory and security, but which scheme is the most effective is still debatable.

In this paper, we provide a survey of key management schemes in wireless networks. We notice that no key distribution technique is ideal to all the scenarios where networks are used; therefore the techniques employed must depend upon the requirements of target applications and resources of each individual network..

1. INTRODUCTION

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats.

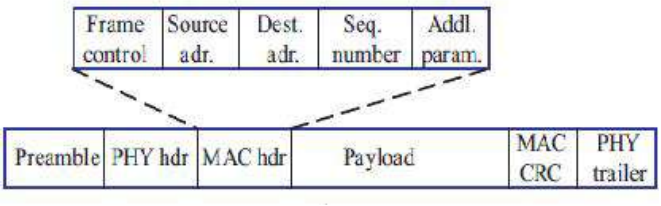

Fig 1: A generic frame format for a wireless network

We consider a sophisticated opponent who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his interior knowledge for initiation discerning blocking attacks in which specific messages of high importance are

targeted.For, a jammer can target route-request route-reply messages at the routing layer to stop route discovery, or target TCP acknowledgments in a TCP session to severely destroy the throughput of an end-to-end movement. To launch perceptive blocking attacks, the adversary must be capable of implementing 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 improving 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 . Discerning blocking requires an intimate knowledge of the physical layer, as well as of the specifics of upper layers.

The key establishment technique for an secure application must minimally incorporate authenticity, confidentiality, integrity, scalability, and flexibility.

Authenticity: The key establishment technique should guarantee that the communication nodes in the network have a way for verifying the authenticity of the other nodes involved in a communication, i.e., the receiver node should recognize the assigned ID of the sender node.

Confidentiality: The key establishment technique should protect the disclosure of data from unauthorized parties. An adversary may try to attack a sensor network by acquiring the secret keys to obtain data. A better key technique controls the compromised nodes to keep data from being further revealed.

Integrity: Integrity means no data falsification during transmissions. Here in terms of key establishment techniques, the meanings are explained as follows. Only the nodes in the network should have access to the keys and only an assigned base station should privilege to change the keys. This would effectively prevent unauthorized nodes from obtaining knowledge about the keys used and preclude updates from external sources.

Scalability: Efficiency demands that sensor networks utilize a scalable key establishment technique to allow for then variations in size typical of such a network. Key establishment techniques employed should provide high-security features for small networks, but also maintain these characteristics when applied to larger ones.

2. PROBLEM STATEMENT

Consider the scenario depicted fig 2 in Nodes A and B communicate via a wireless link. Within the communication range of both A and B, there is a jamming node J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J’s ability to perform selective jamming. Our goal is to transform a selective jammer to a random one. Note that in the present work, we do not address packet classification methods based on protocol semantics, as describe.

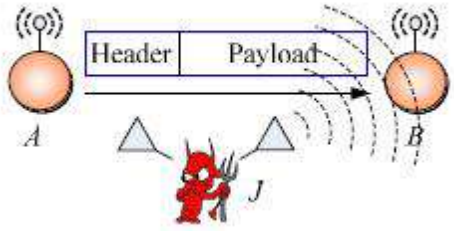

fig 2: Realization of a selective jamming attack

A. Network model

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 presaged pair wise keys or asymmetric cryptography.

B. Adversary Model

We assume the adversary is in control of the communication medium and can jam messages at any part of the network of his choosing. The adversary can operate in fullduplex mode, thus being able to receive and transmit simultaneously. This can be achieved, In addition, the adversary is equipped with directional antennas that enable the reception of a signal from one node and jamming of the same sign allots another. For analysis purposes, we assume that the adversary can proactively jam a number of bits just below the ECC capability early in the transmission. He can then decide to irrecoverably corrupt a transmitted packet by jamming the last symbol. In reality, it has been demonstrated that selective jamming can be achieved with far less resources. A jammer equipped with a single half-duplex transceiver is sufficient to classify and jam transmitted packets.

In particular, he can be equipped withspecial purpose hardware for performing cryptanalysis or any other required computation. Solving well-known

hard cryptographic problems is assumed to be time consuming. For the purposes of analysis, given a cipher text, the most efficient method for deriving the corresponding plaintext is assumed to be an exhaustive search on the key space. The implementation details of every layer of the network stack are assumed to be public. Furthermore, the adversary is capable of physically compromising network devices and recovering stored information including cryptographic keys, PN codes, etc. This internal adversary model is realistic for network architectures such as mobile ad hoc, mesh, cognitive radio, where network devices may operate unattended, thus being susceptible to physical compromise.

3. Real Time Packet Classification

Consider the generic communication system depicted in Fig. At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, DE interleaved, and decoded, to recover the original packet m. Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification. This is because for computationally efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is aware

of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packet to classify it.

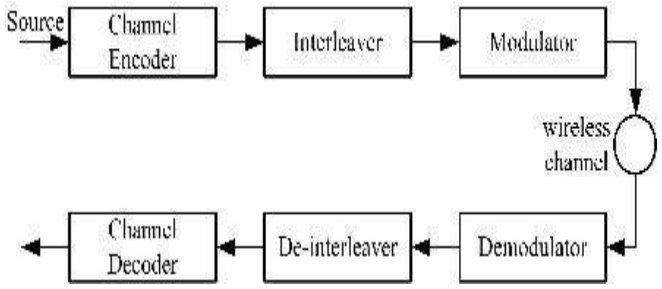

Fig 3: classification of real time packet

4. A STRONG HIDING COMMITMENT SCHEME (SHCS)

We propose a strong hiding commitment scheme, 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. Assume that the sender S has a packet m for R. First S construct (C,d)=commit(m),where

$$C=E_k(\pi_1(m)), d=k.$$

Here the commitment function Ek() is an off the shelf symmetric encryption algorithm,π1 is a publicly known permutation and k is a randomly selected key of some desired key length s. The sender broadcasts (C//d), where "//" denotes the concatenation operation. Upon reception of d, any receiver R computes

$$m = \pi_1^{-1}(D_k(C)),$$

where π1 -1 denotes the inverse permutation of π1. To satisfy the strong 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.

5. 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 predefined 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. 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 overheads.

Let a sender S have a packet m for transmission. The senders select a random key k of 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 o f 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(π1(m)). At the receiver side, any receiver R solves the received puzzle P1 to recover key k1 and then computes m
1= π1 -1(Dk(C)). If the decrypted packet m1 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 m1 =m. Else, the receiver discards m1. Fig. 4 show the details of CPHS.

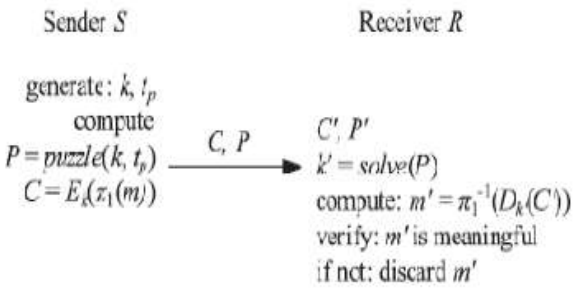

Fig 4: The cryptographic puzzles-based hiding scheme

6. AN AONT-BASED HIDING SCHEME (AONT-HS)

We propose a solution based on All-or-Nothing Transformations that introduces a modest communication and computation overhead. Such transformations were originally proposed by Rivets to slow down brute force

attacks against block encryption algorithms. An AONT serves as a publicly known and completely invertible preprocessing 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 m1=(m1…..mx), is an AONT if 1) f is a bijection, 2) it is

computationally infeasible to obtain any part of the original plaintext, if one of the pseudo messages is unknown, and 3) f-1 and its inverse are efficiently computable. Packets are preprocessed by an AONT before transmission but remain unencrypted. 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. Fig 5 show the details of AONTHS.

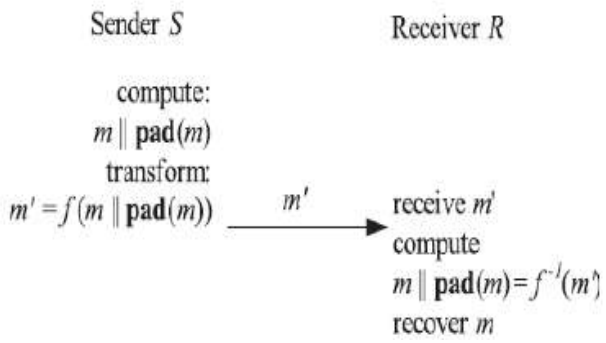

Fig.5.The AONT-based hiding scheme.

7. RANDOM KEY DISTRIBUTION

We propose the use of random key distribution to hide the location of control channels in time and/or frequency. We evaluate performance metrics of resilience to control channel jamming, identification of compromised users, and delay due to jamming as a function of the number of compromised users.

8. PROPOSED WORK

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization. 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 predefined 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. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is infeasible — this is the "elliptic curve discrete logarithm problem" or ECDLP. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplicand given the original and product points. The size of the elliptic curve determines the difficulty of the problem. We Design a new enhanced ECS for Advanced Secured Transmission of data in WSN. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key – e.g., a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key. For current cryptographic purposes, an elliptic curve is a plane curve over a finite field (rather than the real numbers) which consists of the points satisfying the equation.

$$y^2 = x^3 + ax + b,$$

along with a distinguished point at infinity, denoted ∞. (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.)

9. CONCLUSION

In this paper the problem of selective jamming attacks in wireless networks has been addressed and 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. Schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical layer characteristics and analyzed the security of our schemes and quantified their computational and communication overhead. With these schemes a random key distribution has been implemented to more secure the packet transmission in the wireless networks.Here we use elliptic curve cryptography to provide more security. Over the last five years, elliptic curve cryptography has moved from being an interesting theoretical alternative to being a cutting edge technology adopted by an increasing number of companies. There are two reasons for this new development: one is that ECC is no longer new, and has with stood a generation of attacks; second, in the growing wireless industry.

10. REFERENCES

[1] T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130,2006.

[2] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti- Jamming Techniques in Sensor Networks," IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007.

[4] W. Xu, W. Trappe and Y. Zhang, "Anti- Jamming Timing Channels for Wireless Networks," Proc. ACM Conf . Wireless Network Security (WiSec), pp. 203-213, 2008.

[5] R. Rivest, "All-or-Nothing Encryption and the Package Trans- form," P roc . Int'l Workshop Fast Software Encryption, pp. 210- 218,1997.

Author Details

Miss. A. MADHURI, B.Tech Computer Science & Engineering from AITS, Rajampeta and Pursuing M.Tech., Computer science and engineering in Bharath College of Engineering and Technology for Women, Kadapa, AP,

Email: anupatimadhuri@gmail.com

Ms. S RAJIYA SULTANA received the M.Tech degree from Lords, Hyderabad. She published several papers National and International and attended several conferences. She is working as a Assistant professor in Bharath College of Engineering and Technology for Women, Kadapa, AP, Her current research area includes Mobile Computing, Computer Network and Data Mining etc.