ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Establishing Adversary Resistant Communication in Wireless Network

Sona G[1], Annapandi P[2], Addlin Shinney[3]

M.Tech, Department of IT, Dr. Sivanthi Aditanar College of Engineering, Tuticorin, Tamil Nadu, India[1, 3]

HOD, Department of IT, Dr. Sivanthi Aditanar College of Engineering, Tuticorin, Tamil Nadu, India [2]

ABSTRACT: Previously Spread Spectrum (SS) communication involve by setting up preconfigured keys among the communicating nodes that are constrained to possess synchronous behaviour. This extends to several issues creating circular dependency problem, offering less energy efficiency and thereby leading to insecure short-lived communication. In this paper, an opponent resilient secret sharing concept is introduced without any establishment of pre-shared keys by IFEB (Intractable Forward and Efficient Backward) decoding. It illustrates using time reversed message extraction and key scheduling at receiver side that enables secured transmission over wireless communication even when the receiver node remains inactive and attaining jammer not to obtain the original data sent by the sender node. Spreading the data involves use of DSSS as it would be more compatible in adjusting to multiple bandwidths. Main goal is to transmit the message in such a way that the time required to deliver the secret must be less than the time for the opponent to find key during transmission. Further, it come up with minimal storage overhead, cost effective and sustains long-lived secured communication among the interacting nodes. Evaluation of various parameters is performed using NS-2 toolkit to prove that this newer approach is better than earlier work.

KEYWORDS: Direct sequence spread spectrum, zero pre-shared secret, intractable forward and efficient backward decoding, anti-jamming, message extraction, key scheduling.

I. INTRODUCTION

Electro-magnetic waves are the key source for establishing radio-frequency communication. With this it is not only possible for ultimate nodes to communicate instead it can also be available for adversaries. The ability to recover back from malicious attack is obviously an important characteristic for military communication during a battle-field. It is also gaining importance in civilian and commercial applications due to the increased trust on wireless networks for connectivity to the cyber network infrastructure and applications that monitor our environments such as tunnels, bridges, landmarks, buildings, etc. For several decades jamming and anti-jamming techniques were handled for the physical layer of wireless systems supporting mostly voice communication. However, it is only recently that the networks with complex medium sharing and application protocols opened the door for sophisticated attacks and resulted in the exploration of new recover back mechanisms.

The paper illustrates a new paradigm for breaking the anti-jamming key establishment circular dependency with significant energy efficiency advantages over UFH. Our mechanism depends on two main properties:

a) Intractable Forward Decoding (IFD, preventing an adversary from detecting or decoding an on-going communication)
b) Efficient Backward Decoding (EBD, allowing any receiver to decode the time-reversed signals)

The key advantage of our result, in comparison with UFH, is that it does not require excess energy for transmitting packets. It is in fact as energy efficient as the conventional SS communication where the communicating nodes require pre-sharing of a secret key. UFH, on the other hand, requires on average *n* times more energy than conventional SS, *n* being the spreading factor that is in the order of hundreds. We achieve this communication-energy efficiency with a little increase in the receiver computation and storage cost.

The working of this paper is both conceptual and algorithmic:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Zero communication-energy overhead key establishment of a shared key without pre-agreed knowledge (in comparison with conventional SS with pre-shared keys): a novel approach based on intractable forward-decoding and efficient backward-decoding.

1) Undetectable communication until end of transmission (delayed detection) forcing the jammer to become energy-inefficient and channel-oblivious.
2) A destination-oriented scheme that prevents efficient simultaneous-attacks on multiple receivers.

II. CONSIDERATIONS OF WCN

Consider a wireless communication network where several nodes are trying to establish pairwise-shared secret that would enable SS communication. This focuses on a pair of communicating nodes along with a jammer, all sharing a RF channel. The jammer's objective is to prevent the establishment of the secret key between the communicating nodes, because once this key is established; the communicating nodes can use conventional SS for communication making them resilient to jamming. The main objective is to devise a jammer-resilient message-delivery mechanism with no pre-shared information. Now consider the same MAKAP, namely Elliptic Curve Diffie Hellman (ECDH) because of the small number of messages exchanged (two) and their short length. Our method uses Direct-Sequence SS (DSSS), but it easily generalizes to Frequency-Hopping SS (FHSS).

III. TIME REVERSED MESSAGE EXTRACTION AND KEY SCHEDULING

Hence the main aim of this paper is

- To determine and identify the improvement that can be made in evaluating the influence of jammer not to obtain the information while communication is in progress.
- To evaluate Packet Loss Rate (PLR), False Positive (FP), computation and storage cost for establishing energy efficient Spread Spectrum communication.

Node Creation

Our communication model consists of sender, receiver where they share the same channel and information such as MAC addresses, key lengths, communication Protocol, and encoding/decoding schemes. In addition to this, we consider that the jammer too lies on the same channel. As our communication is extensively large we use Spread Spectrum (SS) communication model for spreading and transmitting data. Multiple nodes are created in this paper to create a suitable environment for transferring data from multiple sources.

Intractable Forward Decoding (IFD)

Both the data and secret key utilizes the cryptographic PN Sequence. With this, it is necessary to find the jammer resiliency and energy efficiency. The packet data bits are spread from the source and estimate the total energy per packet. Spreading a signal by a factor allows the communicating nodes to counter an n-times stronger jammer at no extra energy cost to the sender. Hence, it need to scale jamming energy J by the same factor maintain the same BER.

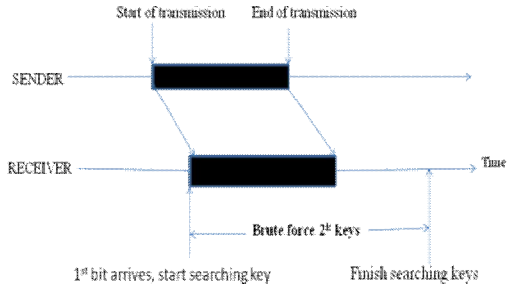

Figure 2. Intractable Forward Decoding

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The working of this module is shown in Figure 2. Main goal is to transmit the message in such a way that the time required to deliver the secret must be less than the time for the opponent to find key during transmission.

Time Reversed Message Extraction and Key Scheduling (TREKS)

Then finding the keys generated by the cryptographic PN Sequence. First scheduling the keys and protects against brute force search of the key. Schedule a key in a sequence of order. The every key is derived; form a significant bit. Partition the message into a segment depends upon the size of a message. Each segment is spread with a PN sequence derived cryptographically from key sequence. After the jamming the key entropy is same according to the key size. So denote the transmission time respect to the key size and sequence order. The data transfer is started by splitting the message into the various partitions. First transmit the one partition and other half of the message partition sends again for providing the secure transmission. Because the value of Mask bits is public information, the jammer may use it to spread its signal and jam the last bit of the packet. To avoid this, the sender can use the destination's MAC address as the value of Bits. A key entropy decrease; Key Scheduling protects every segment against brute forcing, and thus the entire message. For protecting cryptographically secure PN generators such as ones based on AES-128.

Key Scheduling Algorithm:

A sequence of keys that is $K_1, K_2, ..., K_n$ is known as schedule by setting i-1 MSB to some i-1 arbitrary value C. To spread keys we partition message into *k* segments that are derived cryptographically from K_i. The symbols used to illustrate key scheduling process are described in Table 1.

Notation	Definition
PN (.)	PN generating function
K_i	i^{th} key in the schedule
K[m,.., n]	K^{th} substring from m to n bit
M[m,.., n]	M^{th} substring from m to n bit

Table 1. Symbols used for Key Scheduling

The key scheduling algorithm is described in given below

routine TRANSMITTER (M, K)
N1 ← M
for i= 1,..,k **do**
K_i[i,..,k] ← K[i,..,k]
K_i[i,..,i-1] ← C[i,..,i-1]
M_i ← N_i [1,..,| N_i|/2]
PN_i ← PN (K_i)
Disperse M_i with PN_i
N_{i+1} ← N_i[|M_i|+1,..,| N_i|]
end for
end routine

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Efficient Backward Decoding (EBD)

Efficient Backward Decoding, the receiver can deduce the key, due to the decreasing key entropy, by guessing two keys to find the end of transmission. The receiver does not have the same time constraints as the jammer; he can store the received signals, and then process them backwards in time. The EBD mechanism is shown in Figure 3.

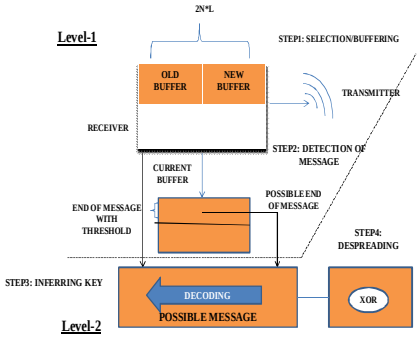

Figure 3 Efficient Backward Decoding

Level 1 consists of finding the EoM by computing the cross correlation between the received spread signal and the PN-sequence generated with the receiver's MAC address. In Level 2, the receiver infers the key in reverse time, starting where the high correlation was detected in level I. If correlation is maintained in time, then the key has been found, and the message is dispreads. When new signal samples arrive, the receiver enqueues them into a FIFO order.

The use of this algorithm enables to establish long term spread spectrum communication without any pre-configured key concept. With this accomplishment, it is possible for the sender and receiver to infer the spreading key in regular order.

IV. RESULTS AND DISCUSSION

Average Delay

Delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Thus, the formula for computing delay is

Delay = Receiving Time – Sending Time

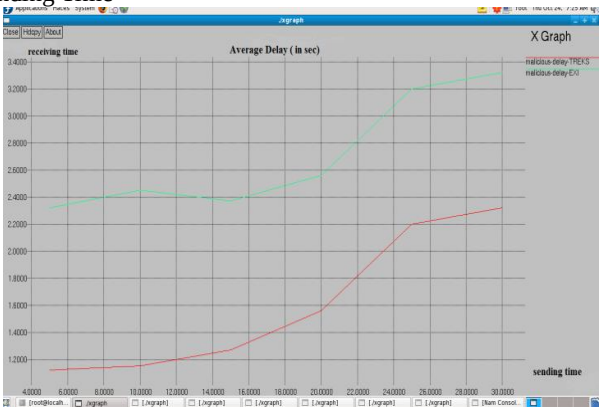

Figure 4 Average delay

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

In the presence of attacker/malicious behavior, using TREKS method the average delay is significantly reduced in comparison with normal transmission of packets between nodes in the network. The result obtained is shown in Figure 4.

Data Transmission

Packet Delivery Ratio is the ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender. This is computed using the following formula

PDR = ∑ Number of packet receive / ∑ Number of packet sent

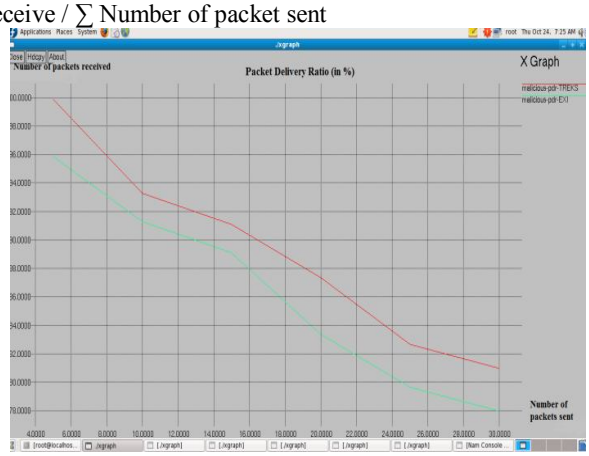

Figure 5 Packet delivery ratio

In the presence of attacker/malicious behaviour, using TREKS method the packets are delivered in higher order than with normal transmission of packets between nodes in the network. The result is shown in Figure 5.

False Detection Ratio

False Detection Ratio represents the number of false susceptive (here malicious act) relative to the total number amount of decision (their identity). Formula to compute FDR is shown below

FDR = No of Malicious node given/ No of Malicious identity

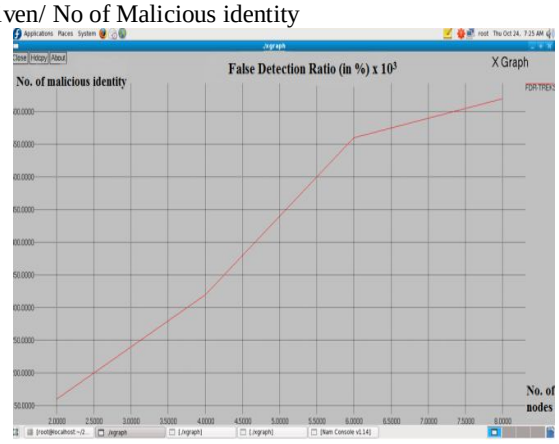

Figure 6 False detection ratio

The ability in identifying and making resilient about the attack in data is computationally high using TREKS method which is shown in Figure 6.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Routing Overhead

Routing Overhead is calculated by dividing the total number of routing packets sent (includes forwarded routing packets as well) by the total number of data packets received. It is computed using the following formula

Routing Overhead = Total no of Routing Packet/ No of data Packet Received

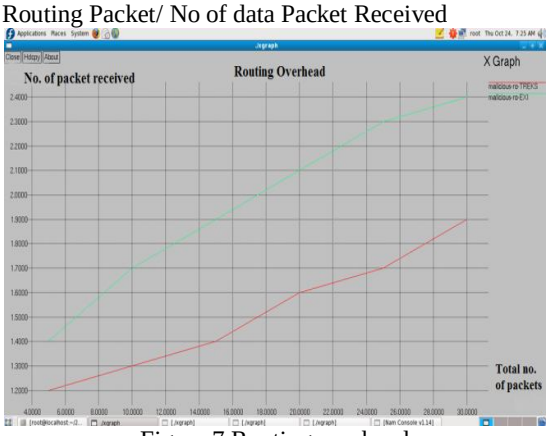

Figure 7 Routing overhead

In the presence of attacker/malicious behaviour, using TREKS method the Routing Overhead is significantly reduced than normal transmission of packets in the network. The result is shown in Figure 7.

V. CONCLUSION

The work introduces a method for achieving SS anti-jamming without a pre-shared key. The method has zero energy overhead in comparison with conventional SS communication. Main solution relies on Intractable Forward Decoding and Efficient Backward Decoding. The utilisation of several algorithms helps to optimize the decoding and show that the computational cost of despreading is less than twice the conventional SS cost. Also, the method has additional benefits of delayed detection and destination-oriented transmission making jamming infeasible and keeping its impact to minimal by prohibiting jammers from simultaneously jamming multiple receivers.

In addition to this, it enables establishing a SS system against jamming without pre-shared secret, zero energy overhead in comparison to traditional SS system. Also, TREKS Computation cost ≤ 2 * traditional SS communication cost allowing destination-specific transmission and inability to detect packet.

REFERENCES

[1] P. Tague, M. Li, and R. Poovendran, "Probabilistic Mitigation of Control Channel Jamming via Random Key Distribution," Proc. IEEE 18th Ann. Int'l Symp. Personal, Indoor, and Mobile Radio Comm. (PIMRC), 2007.

[2] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, "Jamming Resistant Key Establishment Using Uncoordinated Frequency Hopping," Proc. IEEE Symp. Security and Privacy (ISSP), 2008.

[3] C. Popper, M. Strasser, and S. Capkun, "Jamming-Resistant Broadcast Communication without Shared Keys," Proc. USENIX Security Symp., 2009.

[4] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks," Proc. IEEE INFOCOM, 2010.

[5] J. Chiang and Y.-C. Hu, "Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks," Proc. ACM MobiCom, 2011.

[6] G. Lin and G. Noubir, "On Link Layer Denial of Service in Data Wireless LANs," Wireless Comm. Mobile Computing, vol. 5, no. 3, pp. 273-284, 2005.

[7] S. Gilbert, R. Guerraoui, and C. Newport, "Of Malicious Motes and Suspicious Sensors: On the Efficiency of Malicious Interference in Wireless Networks," Proc. Int'l Conf. Principles of Distributed Systems (OPODIS), 2006.

[8] K.B. Rasmussen, S. Capkun, and M. Cagalj, "SecNav: Secure Broadcast Localization and Time Synchronization in Wireless Networks," Proc. ACM MobiCom, 2007.

[9] B. Awerbuch, A. Richa, and C. Scheideler, "A Jamming-Resistant MAC Protocol for Single-Hop Wireless Networks," Proc. 27th ACM Symp. Principles of Distributed Computing (PODC), 2008.

[10] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the Performance of IEEE 802.11 under Jamming,"Proc. IEEE INFOCOM, 2008.