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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Secure Energy Efficient Routing Using Jamming To Resist Networking Eavesdroppers

Sheetal Modke, Prof. Pradnya Kasture

M.E, Dept. of Computer, RMD Sinhgad School of Engineering, Savitribai Phule University, Pune, Maharashtra, India.

Professor, Dept. of Computer, RMD Sinhgad School of Engineering, Savitribai Phule University, Pune, Maharashtra, India

ABSTRACT: The proposed system is designed to implement a safe energy efficiency path in the presence of passive interceptor. The foregoing work in this area is believed to be sure that the situation and information about the location of each interceptor channel is considered safe. However, in the wireless network, the position of passive interceptors and CSI is not known, making it difficult to guarantee confidentiality for a routing algorithm. The proposed system improves the coding of the energy-efficient network for secure transmission in the network. We develop an effective path algorithm that is not based on interceptor status and any information about CIS. Using the additive random block is a key to utilizing the recipient's built-in non-motivations so that the interceptor cannot record messages. Our results show that when uncertainty in case of failure is high and / or deprived of wireless environment, our algorithm is more than the existing algorithm regarding energy consumption and privacy. We present protocols for creating secret pairs of essays between nodes in a wireless network, so these secrets are protected from an interceptor, under standard theoretical hypotheses; our protocol is protected by theoretical information. Secondly, we offer a secret protocol for arbitrary multi-hop networks based on the original protocol, but additional resources for privacy, including design features to utilize multi-hop offers.

KEYWORDS: Network security, Wireless networks, Quantization, Routing protocols, Energy-aware systems, Secret key generation, packet erasures

I. INTRODUCTION

Information secrecy has been accomplished by cryptography, which depends on suspicious on present and future computational capacities of the enemy. The design of algorithms to provide secrecy in networks of arbitrary "moderate" size is of interest, which is considered here. We consider a network with multiple system nodes where a source node communicates with a destination node in a multi-hop fashion and in the presence of multiple passive eavesdroppers. We define the cost of communication to be the total energy spent by the system nodes to securely and reliably transmit a message from the source to the destination. Thus, our goal is to find routes that minimize the cost of transmission between the source and destination nodes. Energy efficiency is an important consideration in designing the routing algorithms. The existing routing algorithm is called SMER (secure minimum energy routing) which employs cooperative jamming to provide secrecy at each hop such that the end-to-end secrecy of the multi-hop source-destination path is guaranteed. But, the energy consumption of any cooperative jamming approach can become very high.

In this paper, we address the multi-hop network in the presence of multiple eavesdroppers with unknown locations and CSIs. Also, we consider a more realistic wireless setting, and design an efficient (polynomial time) routing algorithm such that the aggregate energy spent to convey the message and to generate the random jamming signal is minimized.

DOI: 10.15680/IJIRCCE.2017. 0512022

II. LITERATURE SURVEY

The paper [1] proposes wiretapper for searching available network link for free to communicate. The no uniform case, this secrecy rate is achievable for the case of known but not unknown wiretap set. Determine high secrecy rate for packet transmission over network. Network flow management.Advantage: Achieves high secrecy rate. Secure communication via injected node to maintain efficient communication link. The paper [2] describes four fundamental channel models: 1) Gaussian wiretap channel; 2) Gaussian broadcast channel with confidential messages; 3) Gaussian interference channel with confidential messages; and 4) Gaussian multiple access wiretap channel. An upper bound that relates the entropy of the cooperative jamming signal from the helper and the message rate. An achievable scheme based on real interference alignment which aligns the cooperative jamming signal from the helper in the same dimension as the message signal. Advantages: Highest differential entropy. Reliable decoding at the legitimate receiver.

A protocol for secret communication between a source and destination using a messaging relay and artificial noise transmitted from a set of intervening relays has been presented in paper [3]. The system exploits a multi-user effect in selecting both the messaging relay and the nodes for noise generation. The proposed protocol significantly outperforms approaches based on standard multi-user diversity. Advantages: The number of eavesdroppers that can be tolerated while a packet is transmitted secretly with high probability. The proposed approach significantly outperforms a power control approach based on standard multi-user diversity. The papers [4] proposes two-hop strategy for the case of equal path-loss between all pairs of nodes, and then consider its embedding within a multi-hop approach for the general case of an extended network.A protocol for two-hop communication between a large numbers of source-destination pairs via one relay for each pair is proposed. A two-hop strategy for the case of equal path-loss between all pairs of nodes, and then considers its embedding within a multi-hop approach for the general case of an extended network. Advantages: Finds the maximum achievable number of eavesdroppers that can be tolerated while maintaining reliability and secrecy. Achieves higher bandwidth efficiency.

The paper [5] proposes active cooperative relaying based schemes. To allow *arbitrary* cooperation among legitimate nodes in deriving scaling laws for large wireless networks with secrecy constraints. To achieve this result, we make use of (i) block Markov DF relaying, (ii) Wyner’s wiretap coding at the source, in order to secure the new part of the message transmitted in each block, and (iii) beamforming, to secure the coherent parts transmitted cooperatively by all the nodes in the network. Advantages: Cooperation based schemes can achieve secure communication with cost that goes to 0. To obtain the eavesdroppers’ CSI.

Traditionally, information has been obtained through confidentiality cryptography which is based on current and future computing capabilities of the contestant. However, there are many examples of cryptographic scammatics that question for being corrupt. This is the case when an enemy is the way the channel is trying to listen to the main channel between transmitter and receptionist to achieve a positive level then the main channel is by privacy, Supervisors are unknown and may be close to the sender, but the recipient receives the suspect. In wireless environments, many uninspired emails have big uncertainty in resellers trying to see the messages on every jump, because the label spreader, and e-mails. Inversion for transmitters can be discontinued. In this case, consumption of energy may be very high in case of interference with any cooperative. Wrong numbers of listeners or, apparently, speaker channels violate the privacy secret.

Disadvantages:

1. Multiple eavesdroppers may be trying to intercept the message at each hope.
2. In wireless networking eavesdroppers changes the locations so could not identify the exact eavesdropper.
3. Energy consumption and computational complexity is high.
4. Network secrecy is less.

III. PROPOSED SYSTEM APPROACH

In a multi-hop network in the presence of multiple eavesdroppers with unknown locations and CSIs. Also, we consider a more realistic wireless setting, and design an efficient (polynomial time) routing algorithm such that the aggregate energy spent to convey the message and to generate the random jamming signal is minimized.In the modeling of the point-to-point links in the network, consider a more realistic wireless communication environment compared to the line-of-sight communication considered in the point-to-point method by: (a) incorporating multi-path fading in modeling and analysis; (b) in contrast to secrecy approaches that consider perfect jamming cancellation at the legitimate receive, considering the channel estimation error which causes an error in the cancellation of the jamming signal at the intended receiver.

We develop an optimization framework to minimize the amount of energy that is used by the random jamming technique to convey a message reliably and securely from a source node to a destination node in a multihop fashion.We show that secure and reliable multi-hop communication is possible in an arbitrary network, even in the presence of multiple eavesdroppers of unknown number, locations and CSIs. The critical challenge in providing physical layer secrecy in wireless networks, especially in the case of passive eavesdroppers with unknown locations and CSIs, can be resolved using the random jamming technique.

We show that the algorithm developed from the random jamming approach coupled with our approach to network optimization: (a) has improved performance in different scenarios compared to other approaches (i.e. SMER); (b) has performance that is independent of the particular statistical distribution of the channel gain between the transmitter and the eavesdropper, and thus will work for any kind of eavesdropper's channel.

Our contribution work is to design protocols that exploit packet erasures, in order to enable each pair of terminals in the network, to create a secret that is secure from an adversary model.

Advantages:

1. Minimize the energy consumption.
2. It provides physical layer secrecy in wireless networks.
3. It provides reliable and secure message transfer from source node to the destination node.

- **System Architecture:**

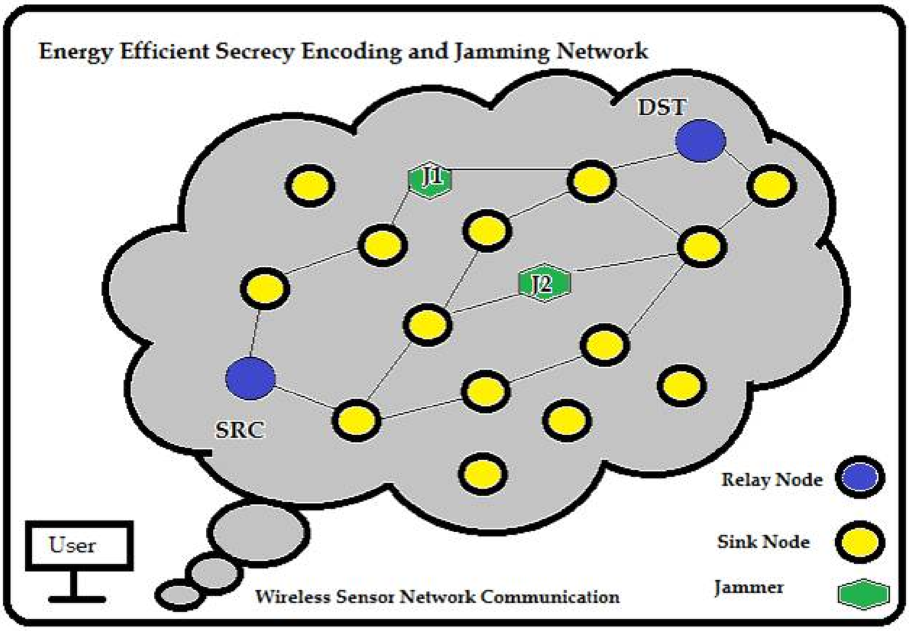
Energy Efficient Secrecy Encoding and Jamming Network
DST
J1
J2
SRC
Relay Node
Sink Node
Jammer
User
Wireless Sensor Network Communication

Fig.1. Proposed system architecture

IV. MATHEMATICAL MODULE

Efficiency captures the cost of the protocol, i.e., the amount of traffic it produces in order to generate pair wise secrets of a given size. The efficiency achieved by two terminals *Ti* and *Tj*that create a secret *Si j*, of length |*Si j* | bits,

Ei j* =|*Si j* |*total transmitted bits

(Number of Erasures= Number of Secrets of packet/ total transmitted bits)

The denominator is the total number of bits transmitted

DOI: 10.15680/IJIRCCE.2017. 0512022

End-to-end Encoding: At every generation of new confidentialmessage, i.e., Let , $P_s(t)=0$, let $k_s(t+1)=k_s(t)+1$,and determine end-to-end confidential encoding rate.

Flow control: At each block, for some, each source injects confidential bits into its queues:

Encoding:-

Representation of each letter in secret message by its equivalent ASCII code.

□ Conversion of ASCII code to equivalent 8 bit binary number.

□ Division of 8 bit binary number into two 4 bit parts. Choosing of suitable letters corresponding to the 4 bit parts.

□ Meaningful sentence construction by using letters obtained as the first letters of suitable words.

□ Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.

□ Encoding is not case sensitive.

Decoding

Steps:

□ First letter in each word of cover message is taken and represented by corresponding 4 bit number.

□ 4 bit binary numbers of combined to obtain 8 bit number.

□ ASCII codes are obtained from 8 bit numbers.

□ finally secret message is recovered from ASCII codes.

Algorithm for packet transmission Sequence:-

```
Input: A recent offset sequence
Output: $VI$: the estimated offset of the source and forwarder
procedure OFFSET-ESTIMATOR
    Let $\omega = (s1 \ldots sn)$ be the offset sequence
    $c\ (VI) = 0$
    for $i = 2$ to length ($\omega$) do
        if $si \equiv si-1$ then
            increase $c\ (vi)$ where $vi = si$
    return $vi$where $c\ (vi)$ is the maximum
```

Multi-hop Routing Algorithm:

```
1: For each node that generate or receives a data packet, such as node A, do
2:      select B as the next hop such that B has never been selected in this data routing process, has the largest trust and is nearer the sink
3:      If A finds such node, for instance, node B
4:           send data packet P to node B
5:           If node B is the sink then
6:                this data routing procession is completed
7:           End if
8:      Else
9:           Send failure feedback to the upper node, such as node C
10:     End if
11: End for
12: For each node that receives failure feedbacks, such as node B, do
13:     Repeat step 2 to step 10
14: End for
```

V. CONCLUSION

To provide confidentiality, developed an energy-efficient router algorithm based on random jamming to exploit e-drip receiver receptors. Our routing algorithm is fast (finds the best way in plural times), and it does not depend on the number of shops and their location and / or state of the information in the channel. We use multi-hope simulation with many network parameters, and the performance of our proposed algorithm. The current work for our best knowledge is to develop protocols for secret key exchange in the Multi-Hop Network, which use the same channel and network assets and to report privacy rates. The proposed algorithm directly addresses one of the major bottlenecks for the implementation of information in formal security in wireless networks: firmness in operating environments.

REFERENCES

[1] Tao Cui, TraceyHo, JörgKliewer ,“On Secure Network Coding With No uniform or Restricted Wiretap Sets”, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 59, NO. 1, JANUARY 2013

[2] J. Xie and S. Ulukus, “Secure degrees of freedom of one-hop wireless networks,” IEEE Transactions on Information Theory, vol. 60, no. 6, pp. 3359–3378, 2014.

[3] D. Goeckel, S. Vasudevan, D. Towsley, S. Adams, Z. Ding, and K. Leung, “Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks,” IEEE Journal on Selected Areas in Communications, vol. 29, pp. 2067–2076, 2011.

[4] A. Sheikholeslami, D. Goeckel, H. Pishro-Nik, and D. Towsley, “Physical layer security from inter-session interference in large wireless networks,” in Proc. IEEE INFOCOM, 2012, pp. 1179–1187.

[5] M. Mirmohseni and P. Papadimitratos, “Scaling laws for secrecy capacity in cooperative wireless networks,” in Proc. IEEE INFOCOM, 2014, pp. 1527–1535.