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. 6, Issue 5, May 2018

Energy Efficient Network Encoding By Creating Secrets of Packet Erasure Using Network Node Is Jamming Randomly

Rupali Tonape[1], Neha Nhayade[1], Kirti Dalvi[1], Gulshan Singh[1], Trupti Dange[2]

B. E Students, Department of Computer Science Engineering, RMD Sinhgad School of Engineering, Pune, India[1]

Professor, Department of Computer Science Engineering, RMD Sinhgad School of Engineering, Pune, India[2]

ABSTRACT: Proposed system is designed to implement secure energy efficient routing in the presence of passive eavesdroppers. Previous work in this area has considered secure routing assuming knowledge of the location and channel state information of each eavesdropper. In wireless networks, however, the locations and CSIs of passive eavesdroppers are not known, making it challenging to guarantee secrecy for any routing algorithm. Proposed system improve energy efficient network coding for secure transmission in the network. We develop an efficient routing algorithm that does not rely on any information about the locations and CSIs of the eavesdroppers. The key is to employ additive random jamming to exploit inherent non-idealities of the eavesdropper's receiver, which makes the eavesdroppers incapable of recording the messages. Our results indicate that when the uncertainty in the locations of eavesdroppers is high and/or in disadvantaged wireless environments, our algorithm outperforms existing algorithms in terms of energy consumption and secrecy.

We present protocols for creating pair wise secrets between nodes in a wireless network, so that these secrets are secure from an eavesdropper, under standard theoretical assumptions, our protocol is information-theoretically secure. Second, we propose a secret-agreement protocol for arbitrary, multi-hop networks that build on the basic protocol but also comprises design features for leveraging additional sources, that multi-hop offers, for secrecy.

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. 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. Here 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 come to be very high.

In this paper, address the multi-hop network in the presence of multiple eavesdroppers with unknown locations and CSIs. Also, 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.

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. 6, Issue 5, May 2018

II. LITERATURE SURVEY

In the paper [1],proposes an ARQ and deterministic network coding as methods of transmission for private and public channel. This paper refers to automatic repeat request, deterministic network coding etc. Advantages are: Efficient packet delivery, Network lifetime increases. Disadvantages are: Node security concerns, delay in packet transmission. The paper [2] proposes a cooperative jamming and decodes and forward for relay transmission approaches. Network relay for cooperative node authentication is used in this paper. Advantage: cooperative relay communication, effective in network jamming problem. Proposes wiretapper for searching available network link for free to communicate in [3]. 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.Advantages are achieves high secrecy rate, secure communication via injected node to maintain efficient communication link. In [4] paper represents securing the network does not entail a loss in the per node throughput. The achievability argument is based on a novel multihop forwarding scheme where randomization is added in every hop to ensure maximal ambiguity at the eavesdropper(s). Packet bit randomization for adding noise to original packet transmission. Advantages are data packet security for network node. Increases throughput for packet randomization.Masked beam forming scheme [5] that radiates power isotropically in all directions.Optimal performance in the high SNR regime. In this paper referred Beam forming scheme for energy power performance increase. Advantage is optimal network performance increases.

Information secrecy has traditionally been achieved by cryptography, which is based on assumptions on current and future computational capabilities of the adversary. However, there are numerous examples of cryptographic schemes being broken that were supposedly secure. In this situation where an adversary tries to eavesdrop on the main channel between a transmitter and a receiver, if the eavesdropper's channel is degraded with respect to the main channel, a positive secrecy rate can be achieved.The locations of eavesdroppers are not known and an eavesdropper might be much closer to the transmitter than the intended receiver.In a wireless environment, many passive eavesdroppers might try to intercept the message at each hop, with large uncertainty in the locations of the eavesdroppers, and the eavesdroppers might get arbitrarily close to the transmitters. In such a situation, the energy consumption of any cooperative jamming approach can become very high.The wrong number of eavesdroppers or do not correctly anticipate the quality of the eavesdroppers' channels, the secrecy will be compromised.

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. SYSTEM DESIGN

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.

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. 6, Issue 5, May 2018

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:**

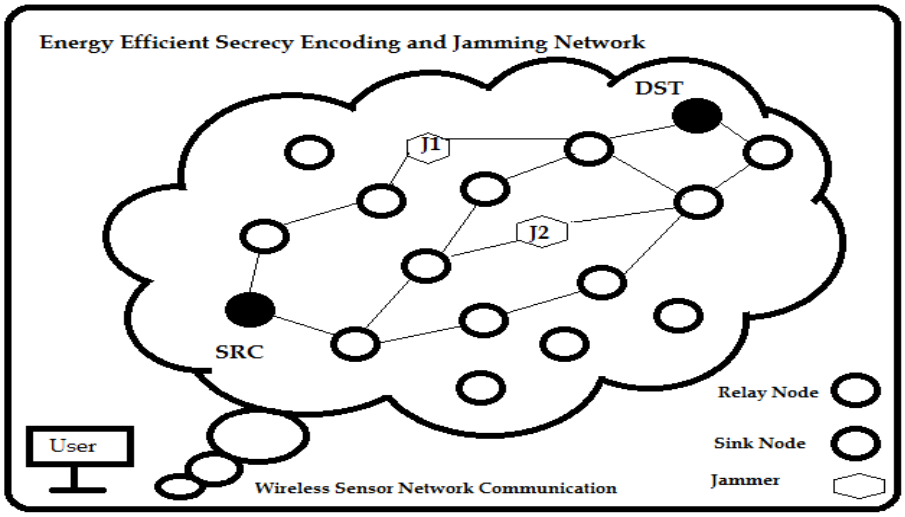

Fig.1. Proposed system architecture

- **Block Diagram:**

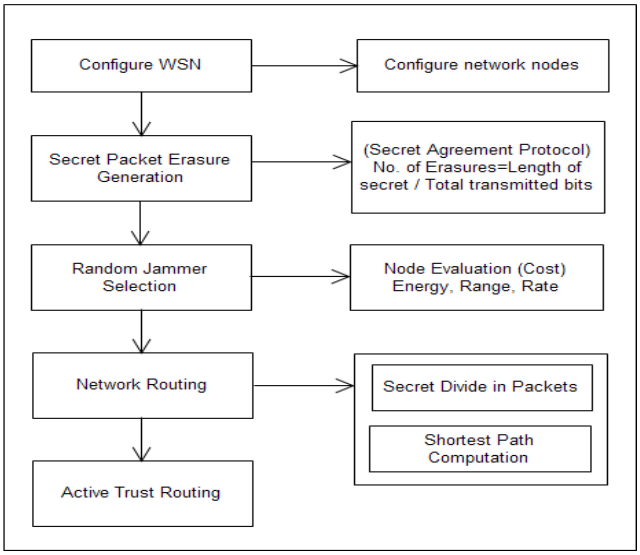

Fig.2. Block Diagram

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. 6, Issue 5, May 2018

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

Euclidean Distance:

$$\mathrm{d}(\mathbf{p},\mathbf{q}) = \mathrm{d}(\mathbf{q},\mathbf{p}) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \cdots + (q_n - p_n)^2}$$

$$= \sqrt{\sum_{i=1}^{n} (q_i - p_i)^2}.$$

Dijkstra's Algorithm Formula:

$$E_q\left(k\tau_z\right) = \sum_{i=1}^{M} E_q\left(t\right) = \sum_{i=1}^{M} \frac{1}{\mu_i - \lambda_i\left(k\tau_z\right)}$$

$$= \sum_{i=1}^{M} \frac{1}{\mu_i - \left(q_{si}\lambda\left(k\tau_z\right) + \sum_{k=1}^{M} q_{ki}\lambda_K\left(k\tau_z\right)\right)}$$

Algorithm and related mathematics:-

We consider wireless networks in which messages are carried between the source destination pairs cooperatively in a multi-hop fashion via intermediate nodes. In a multihop network, as data packets are transferred, intermediate nodes obtain all or part of the information through directly forwarding data packets or overhearing the transmission of nearby nodes. This poses a clear problem when transferring confidential messages.

Math:-

End-to-end Encoding: At every generation of new confidential message, 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.

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. 6, Issue 5, May 2018

Algorithm for packet transmission Sequence:-
Input: A recent offset sequence
Output: *VI*: the estimated offset of the source and forwarder
1: procedure OFFSET-ESTIMATOR
2: Let ω = (*s*1... *sn*) be the offset sequence
3: *c* (*VI*) = 0
4: for *i* = 2 to length (ω) do
5: if *si*≡ *si*−1 then
6: increase *c* (*vi*) where *vi* = *si*
7: return *vi*where *c* (*vi*) is the maximum

Network distributed Scheduling
Input : - Number node, neighbors, connectionLinks
Output: - Network scheduling with distributed network
Step1 :- Calculate Weight for each connection
Step2:- Break connection with similar weight
Step3:- Find node which having multiple connection withFree neighbor
Step4:- While Links.size() Do

```
{
 If links.match(request) Then
 {
  Matched link
 }
 Else
 {
        Send matching request to node
 }
}
```

Step5:-IF request. Match (link) then

```
{
 Send matched reply to node
 Send drop message to free neighbors
}
```

Step6:- If Matched reply from neighbor Then

```
{
 Send drop message to free neighbors
}
```

Step7:- If Drop message Then

```
{
  Acknowledge matched link
Neighbors.Remove (node)
}
```

Step8:-

```
End
```

Shortest Path:-
FunctionDijkstra(*Graph*, *source*):
Create vertex set Q
For each vertex *v* in *Graph*: *// Initialization*
Dist[*v*] ← INFINITY *// Unknown distance from source to v*
prev[*v*] ← UNDEFINED *// Previous node in optimal path from source*

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. 6, Issue 5, May 2018

add*v* to *Q// All nodes initially in Q (unvisited nodes)*

dist[*source*] ← 0 *// Distance from source to source*

While*Q* is not empty:

u ← vertex in *Q* with min dist[u] *// Select source node first*

remove*u* from *Q*

For each neighbor *v* of *u*: *// where v is still in Q.*

alt ← dist[*u*] + length(*u*, *v*)

if*alt*<dist[*v*]: *// A shorter path to v found*

dist[*v*] ← *alt*

prev[*v*] ← *u*

Returndist[], prev[]

Dijkstra's algorithm on a graph with edges E and vertices Vcan is expressed as a function of the number of edges, denoted |E|, and the number of vertices, denoted |V|, using big-O notation. How tight a bound is possible depends on the way the vertex set Q is implemented. In the following, upper bounds can be simplified because $|E|=O(|V|^2)$ for any graph, but that simplification disregards the fact that in some problems, other upper bounds on |E| may hold. For any implementation of the vertex set Q, the running time is in

$O(|E|.T_{dk}+|V|.T_{em})$

Where, T_{dk} and T_{em} are the complexities of the *decrease-key* and *extract-minimum* operations in Q, respectively. The simplest implementation of Dijkstra's algorithm stores the vertex set Q as an ordinary linked list or array, and extract-minimum is simply a linear search through all vertices in Q. In this case, the running time is

$O(|E|+|v|^2) = O(|V|^2)$

V. EXPERIMENT RESULT

Consider a wireless network that consists of n system nodes and eavesdroppers which are distributed uniformly at random positions. Find a secure path with minimum aggregate energy from the source to the destination, using SERJ and SMER. In SMER, for every node, two friendly jammers exist that help the node to establish a secure link. Compute the power consumption of SERJ and SMER versus the uncertainty in the location of the eavesdropper. The result shows that the transmit power using SERJ is independent of the location of the eavesdroppers. But with SMER, as the uncertainty in the location of the eavesdroppers increases the power consumption increases.

TABLE I SIMULATION PARAMETERS

Parameter	value
Network size	7000m*500m
Number of sensor nodes	50,70,100
Propagation type	Round Trip
Routing type	Dijkstra
Packet size	32 Bit
Channel	Wireless

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. 6, Issue 5, May 2018

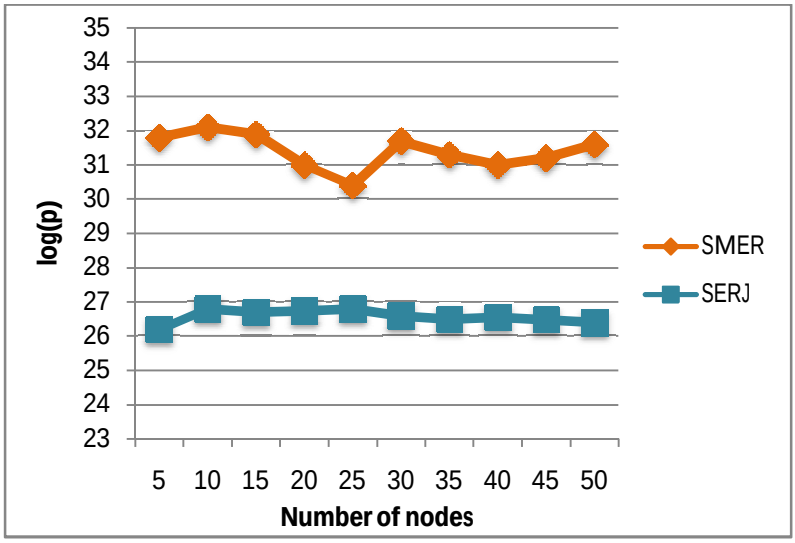

Fig.3 Power consumption of SERJ and SMER versus the number of nodes

Table II Compute power consumption of SERJ and SMER using the no. of nodes

No. of Nodes	SMER	SERJ
5	31.8	26.2
10	32.1	26.8
15	31.9	26.7
20	31	26.75
25	30.4	26.8
30	31.7	26.6
35	31.3	26.5
40	31	26.55
45	31.2	26.48
50	31.6	26.4

VI. CONCLUSION

We developed an energy-efficient routing algorithm based on random jamming to exploit non-idealities of the eavesdropper's receiver to provide secrecy. Our routing algorithm is fast (finds the optimal path in polynomial time), and does not depend on the number of eavesdroppers and their location and/or channel state information. We have performed using simulation of multi-hop networks with various network parameters, and the performance of our proposed algorithm. To our best knowledge the current work is the first to develop protocols for secret key exchange in a multi-hop network that simultaneously exploits channel and network properties, and to report secrecy rates. The proposed algorithm directly addresses one of the key roadblocks to the implementation of information-theoretic security in wireless networks: robustness to the operating environment.

REFERENCES

[1] N. Abuzainab and A. Ephremides, "Secure Distributed Information exchange", IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 60, NO. 2, FEBRUARY 2014
[2] Lun Dong, Zhu Han, Athina P. Petropulu, H. Vincent Poor, "Improving Wireless Physical Layer Security via Cooperating Relays"

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. 6, Issue 5, May 2018

[3] 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
[4] O. OzanKoyluoglu, Can EmreKoksal, Hesham El Gamal "On Secrecy Capacity Scaling in Wireless Networks"IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 58, NO. 5, MAY 2012
[5] AshishKhisti, Gregory W. Wornell, "Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel"