ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

A Novel Approach for Network Secrecy by Generating Secrets of Packet Erasures Using Jammer

Yogita Balram Ahuja, DR. D. P. Gaikwad

Department of Computer Engineering, AISSMS COE, Pune, Maharashtra, India

ABSTRACT: A novel approach is designed to implement energyefficient routing which is secure in the presence of passive eavesdroppers. Previously secure routing considered the information ofeavesdropper such as the location and channel state information.In WSN, the locations and Channel state information of passiveeavesdroppers are unknown. The proposed system improvesenergy efficient network coding for secure transmission in thenetwork. An efficient routing algorithm is implemented that isindependent about the locations and CSIs of the eavesdroppers.Our goal is to deploy additive random jamming to make surethat the eavesdroppers are incapable of recording the messages.The paper represents protocols for generating secrets that arepair wise between nodes in WSN. This is done in order to makesure that these secrets are secure from an eavesdropper. Secondly,a secret-agreement protocol is proposed for multi-hop networksthat is build on the basic protocol. The results show that when theeavesdroppers location is not known our algorithm performs itsbest considering factors such as energy consumption and 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.

Motivation:

1. An energy-efficient routing algorithm based on random jamming to provide secrecy.
2. Effective network communication with hop by hop fashion.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

3. Multipath routing for wireless communication.
4. Message encoding and decoding for automatic authorization.

Objectives:
1. Energy efficient data transmission packet transmission using random jamming.
2. Effective multi hop communication between intermediate nodes with confidentiality.
3. Network packet encoding by creating packet out of packet erasure.
4. Confidentiality preservation by adding noise to message in the form of additional form of bit.
5. Effective and efficient multipath routing.

II. REVIEW OF LITERATURE

N.Abuzainab and A. Ephremides[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. Lun Dong, Zhu Han[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 Tao Cui, TraceyHo, JrgKliewer[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. O. OzanKoyluoglu, Can EmreKoksal[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 AshishKhisti, Gregory W. Wornell[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.
J. Xie and S. Ulukus[6] paper presents 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 are: Highest differential entropy, Reliable decoding at the legitimate receiver. F. Gabry[7], proposesEnergy Efficient Stackelberg game between the two transmitters aiming at maximizing their utilities. Investigate cooperation for secrecy in cognitive radio networks from an energy-efficient perspective. The cognitive transmitter should ensure that the primary message is not leaked to the secondary user by using cooperative jamming. Advantage is to maximize secrecy rate for the primary user. G. Zheng, L.-C. Choo, and K.-K. Wong[8], proposes a distributed implementation algorithm as optimal cooperative jamming. This paper proposes an algorithm to obtain the optimal CJ relay beamforming solution using a combination of convex optimization and a one-dimensional search. A distributed implementation algorithm which permits each individual relay to derive its own weight based on local CSI for achieving a near-optimal secrecy rate. Advantages are: To increase the physical layer security. The optimization of collaborative relay weights for CJ in maximizing the secrecy rate with individual relay power constraints. Disadvantages are: CJ solution is only for one-dimensional search.

A power allocation (PA) policy in I. Krikidis, J. Thompson, P. Grant, and S. McLaughlin[9], that defines how the available power is distributed between the source and the jammer node as well as between the superimposed terms of the DPC design. The proposed scheme enables both the source and the jammer nodes to create intentional

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

interference on the eavesdropper node and significantly improves the achievable secure rate of the system. A PA policy that defines how the transmitted power is split between the source and jammer as well as between the source message and the interference for the DPC based schemes in order to maximize the achievable secrecy. Advantage is the DPC based schemes in order to maximize the secrecy rate. Disadvantage is a non-optimized PA solution limits the achievable secrecy rate of the system.

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 D. Goeckel, S. Vasudevan, D. Towsley[10]. 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 are: 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.

J. Kim, A. Ikhlef, and R. Schober[11] represents, combined relay selection and cooperative beamforming schemes for physical layer security. Cooperative beamforming with multiple relays requires information exchange and synchronization among the different relays so that high operational complexity is induced as the number of relays increases. By reducing the number of participating relays, the array gain obtained from cooperative beamforming is degraded. Advantages are: To minimize the number of relays participating in cooperative beamforming. Minimize the received SNR at the eavesdropper. Better secrecy capacities. Disadvantage is: The direct link from the source to the eavesdropper is ignorable. Y. Zou, X. Wang, and W. Shen[12] proposes the amplify-and-forward (AF) and decode-and-forward (DF) based optimal relay selection (i.e., AF*b*ORS and DF*b*ORS) schemes. Both AF and DF protocols, the proposed optimal relay selection outperforms the traditional relay selection and multiple relay combining approaches in terms of intercept probability. The number of relays increases; the intercept probability performance of both P-AF*b*ORS and PDF*b*ORS significantly improves, implying the wireless security enhancement with an increasing number of cooperative relays. Advantages are: To increase the wireless security against eavesdropping attack. Performance of proposed optimal relay selection is strictly better than that of the traditional relay selection. Disadvantage: Only the single-source and single-destination for cooperative relay networks defend against eavesdropping attack.

The paper [13] elaborates two-hop strategy for the case of equal path-loss between all pairs of nodes, and then considers it's 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 are: Finds the maximum achievable number of eavesdroppers that can be tolerated while maintaining reliability and secrecy. Achieves higher bandwidth efficiency.M. Mirmohseni and P. Papadimitratos[14] 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 are: Cooperation based schemes can achieve secure communication with cost that goes to 0. Obtain the eavesdroppers' CSI.

N. Tekbiyik and E. Uysal-Biyikoglu[15], proposes classification of shortest-path-based energy-efficient routing algorithms designed for wireless ad hoc and sensor networks. Energy efficiency is one of the important design objectives for machine-to-machine network architectures that often contain multi-hop wireless sub-networks. Constructing energy-efficient routes for sending data through such networks is important not only for the longevity of the nodes which typically depend on battery energy, but also for achieving an environmentally friendly system design overall, which will be imperative as M2M networks scale in number of nodes as projected. Advantages are: Energy efficiency, are in the areas of security, privacy, reliability, robustness, latency, cost-effectiveness, software development and standardization. Disadvantage: Scalability.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

III. EXISTING SYSTEM

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.

IV. PROPOSED SYSTEM

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.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

System Architecture:

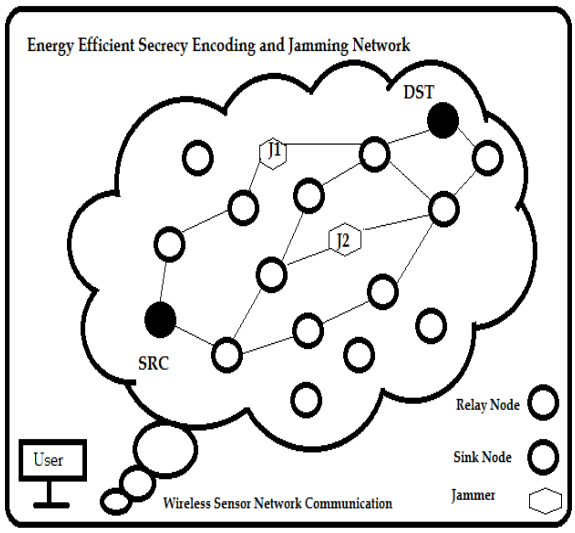

Fig.1. Proposed system architecture

- **Block Diagram:**

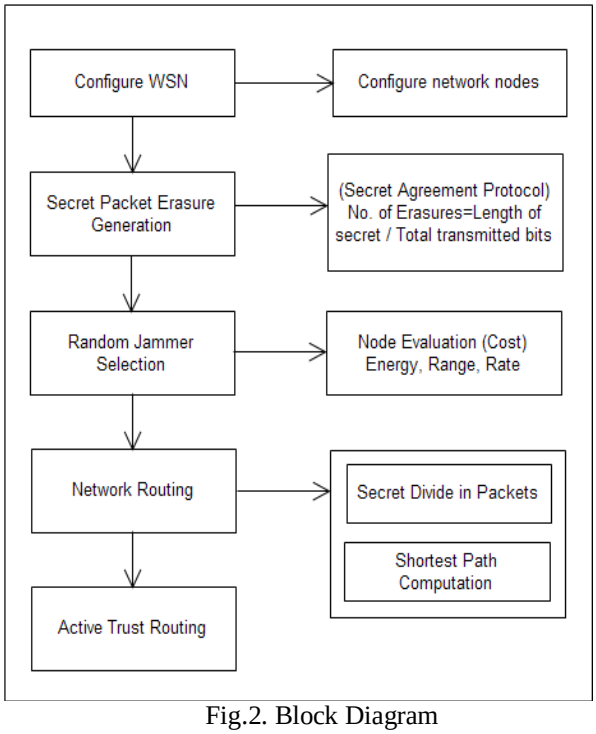

Fig.2. Block Diagram

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

V. MATHEMATICAL MODEL

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:

$$d(p,q) = d(q,p) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \cdots + (q_n - p_n)^2} \qquad = \sqrt{\sum_{i=1}^{n} (q_i - p_i)^2}$$

Dijkstra's Algorithm Formula:

$$E_q(k\tau_z) = \sum_{i=1}^{M} E_q(t) = \sum_{i=1}^{M} \frac{1}{M_i - \lambda_i(k\tau_z)} \qquad = \sum_{i=1}^{M} \frac{1}{M_i - (q_{si}\lambda(k\tau_z) + \sum_{k=1}^{M} q_{ki}\lambda_k(k\tau_z))}$$

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 multi-hop 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:-
Output representation of each letter in secret message by its equivalent ASCII code.
- Conversion of ASCII digit code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts. Choose the suitable letters corresponding to the 4 bit parts.
- Meaningful sentence built 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
1: procedure OFFSET-ESTIMATOR

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

2: Let ω = ($s1$... sn) be the offset sequence
3: c (VI) = 0
4: for i = 2 to length (ω) do
5: if $si \equiv si-1$ then
6: increase c (vi) where $vi = si$
7: return $vi$where c (vi) is the maximum

VI. EXPERIMENT RESULT

Consider a wireless network that consists of n system nodes and eavesdroppers which are distributed uniformly at random positions.The simulation platform used is built using Java language (version jdk 8) on Windows platform. The system does not require any specific hardware to run; any standard machine is capable of running the application.The below table contains the laboring parameters.

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

The evaluation results are carried out considering 50, 70, 90 and 100 nodes respectively. Consider several sources assuming sink nodes and normal sensor nodes respectively. The parameters considered for evaluation are packet delivery ratio (PDR) and throughput ratio.

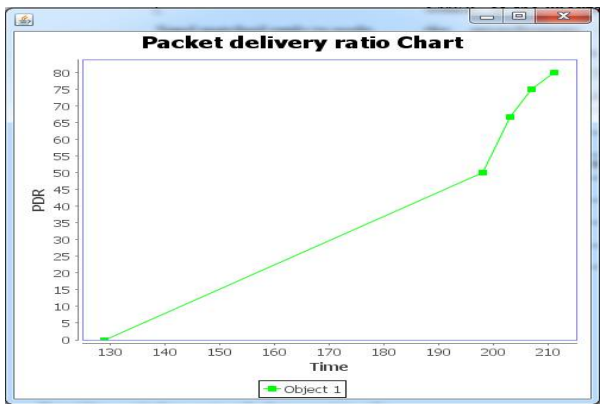

Fig.3 Packet Delivery Ratio Graph

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

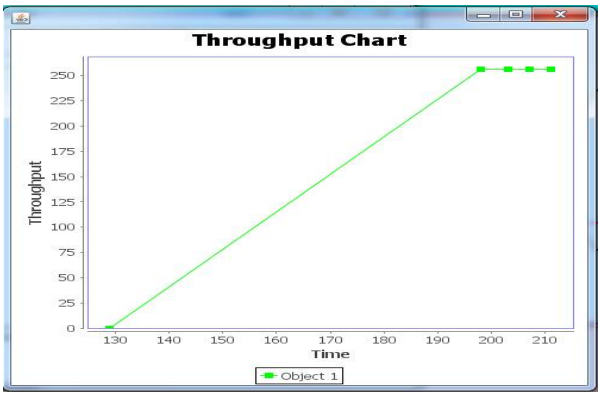

Fig.4Throughput Graph

By observing the above graphs we can conclude that the proposed system gives better results as compared to the existing system in terms of various parameters like packet delivery ratio (PDR) and Throughput ratio.

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.

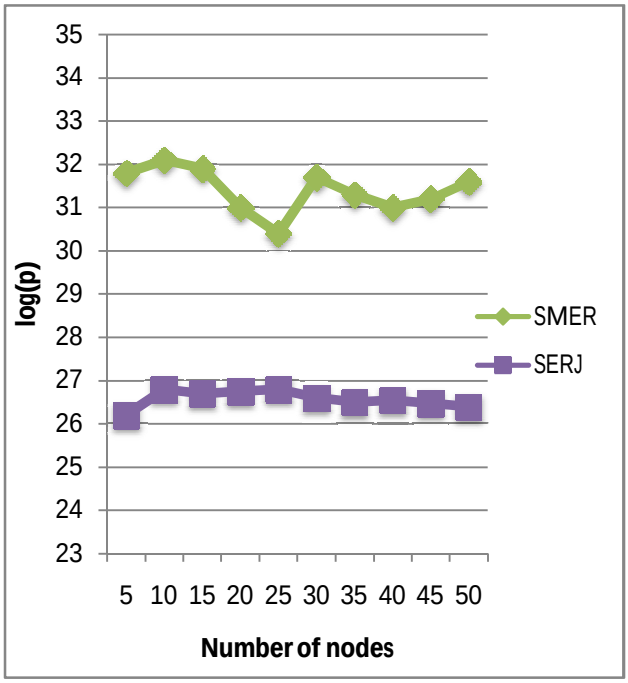

Fig.3 Power consumption of SERJ and SMER versus the number of nodes

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

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

Visit: www.ijirset.com

Vol. 7, Issue 5, May 2018

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

VII. CONCLUSION

We have 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. To our best knowledge the current work is 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"
[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"
[6] 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.
[7] F. Gabry, A. Zappone, R. Thobaben, E. A. Jorswieck, and M. Skoglund, "Energy efficiency analysis of cooperative jamming in cognitive radio networks with secrecy constraints," IEEE Wireless Communications Letters, vol. 4, no. 4, pp. 437–440, 2015.
[8] G. Zheng, L.-C. Choo, and K.-K. Wong, "Optimal cooperative jamming to enhance physical layer security using relays," IEEE Transactions on Signal Processing, vol. 59, no. 3, pp. 1317–1322, 2011.
[9] I. Krikidis, J. Thompson, P. Grant, and S. McLaughlin, "Power allocation for cooperative-based jamming in wireless networks with secrecy constraints," in Proc. IEEE GLOBECOM Workshops, 2010, pp. 1177–1181.
[10] 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.
[11] J. Kim, A. Ikhlef, and R. Schober, "Combined relay selection and cooperative beamforming for physical layer security," IEEE Journal of Communications and Networks, vol. 14, no. 4, pp. 364–373, 2012.
[12] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," IEEE Journal on Selected Areas in Communications, vol. 31, no. 10, pp. 2099–2111, 2013.
[13] 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.
[14] M. Mirmohseni and P. Papadimitratos, "Scaling laws for secrecy capacity in cooperative wireless networks," in Proc. IEEE INFOCOM, 2014, pp. 1527–1535.
[15] N. Tekbiyik and E. Uysal-Biyikoglu, "Energy efficient wireless unicast routing alternatives for machine-to-machine networks," Journal of Network and Computer Applications, vol. 34, no. 5, pp. 1587–1614, 2011.