International Journal on Applications of Information and Communication Engineering
Volume 1: Issue 1: January 2015 , Pages:14-20

Secure Connection in Wireless ad-hoc with Multi-relay Transmission

R.Venkatesharjun[1], P.Bright Prabahar[2]
PG Student,Parisutham Institute of Technology and Science, Thanjavur, Tamilnadu, India[1].
email:arjun88ece@gmail.com
Asst. Prof/ECE Dept,Parisutham Institute of Technology and Science, Thanjavur,Tamilnadu[2].
email:bright.prabahar@gmail.com

Abstract: **In a decentralized wireless networks, confidential message are being transferred from source to destination there is a presence of randomly distributed eavesdroppers. To improve the secure connection probability of direct transmission and relay transmission for colluding eavesdroppers and non-colluding eavesdroppers strategies, where the distributions of relays and eavesdroppers follow homogenous PPPs.**

Keywords: Ad-hoc networks, multi-relay transmission, eavesdropper, Poisson Point Process (PPP)

I. INTRODUCTION

"Ad Hoc" is actually a Latin phrase that means "for this purpose." It is often used to describe solutions that are developed on-the-fly for a specific purpose. In computer networking, an ad hoc network refers to a network connection established for a single session and does not require a router or a wireless base station. A wireless ad hoc network (WANET) is a decentralized type of wireless network. The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding data.

A. Direct transmission:

If the distance between the source and destination is within the transmission range or the coverage range of the base station in wireless ad hoc network, then we go for direct transmission, in which the data should be shared between source and destination directly. That is, there is no intermediate node between source and destination.

B. Relay Transmission

The distance between the source and destination is large when compared with the transmission range of the base station. The data to be shared between the source and destination traverses the intermediate node(s). This type of transmission is called as relay transmission and the message forwarded through relay nodes is called as Hub-by-Hub message transmission. It can be classified into two categories which are as follows.

i.) Serial Relay Transmission is used for long distance communication and range-extension in shadowy regions. It provides power gain. In this topology signals propagate from one relay to another relay and the channels of neighboring hop are orthogonal to avoid any interference.

ii.) Parallel Relay Transmission may be used where serial relay transmission suffers from multi-path fading. For outdoors and non-line-of-sight propagation, signal wavelength may be large and installation of multiple antennas is not possible. To increase the robustness against multi-path fading, parallel relay transmission can be used.

II RELATED WORKS

A. The Relay-Eavesdropper Channel: Cooperation for Secrecy

Our main idea is to exploit user cooperation in facilitating the transmission of confidential messages from the source to the destination. The NF scheme transforms the relay-eavesdropper channel into a compound multiple access channel (MAC), where the source/relay to the receiver is the first MAC and source/relay to the eavesdropper is the second one. R1 is the codeword rate of the source, and R2 is the codeword rate of the relay. We can observe from that if the relay node does not transmit, the perfect secrecy rate is zero for this input distribution since R1(A) < R1(C). On the other hand, if the relay and the source coordinate their transmissions and operate at point B, we can achieve the equivocation rate Re, which is strictly larger than zero. On the other hand, we can still get a positive perfect secrecy rate by operating at point A in the absence of the relay. But by moving the operating point to B, we can get a larger secrecy rate. This illustrates the main idea of our Noise-Forwarding scheme.

Merits

- Multi relay transmission
- Relaying gives more secure connection

Drawback

- Unsecured eves dropper networks.

B. Secrecy in Cooperative Relay Broadcast Channels

We propose an achievable scheme that combines Marton's coding scheme for BCs and Cover and El Gamal's CAF scheme for relay channels. We extend it to include the secrecy rates of the users. Then, we develop a single-letter outer bound on the rate-equivocation region; we accomplish singe-letterization namely by determining suitable auxiliary random variables. Besides this outer bound, for the second user, that is being helped, we develop another single-letter outer bound which depends only on the channel inputs and outputs.

Finally, we consider a Gaussian CRBC and show that both users can have positive secrecy rates through user cooperation. To obtain positive secrecy rates for both users, we provide different assignments for the auxiliary random variables appearing in the achievable rates. These auxiliary random variable assignments have dirty paper coding (DPC) interpretations. In addition, we combine jamming and relaying to provide secrecy for both users when the relaying user is weak.

Merits:

- To avoid the collision attack.
- To reduce time delay.
- No access point and Storage mode may be privacy problem.

C. Characterization of the Secrecy Region of a Single Relay Cooperative System

We characterize the vulnerability region in a single relay cooperative wireless network. Cooperation improves the physical layer security in the network by minimizing the area in which the secrecy capacity is zero. We realize that under certain conditions, this area, called vulnerability region, vanishes. In other words, in this case, we have a perfectly secure system and no matter where the eavesdroppers reside, they will not be able to receive any information intended to the desired destination. This will be possible by carefully designed codes that achieve the secrecy capacity and *without* any key exchange. The improvement in the security is achieved by increasing the capacity of the direct channel by the help of the relay, as well as decreasing the capacity of the eavesdropper channel by introducing interference (jamming) from the relay and the source.

Merit:

- Secure data transmission in single relay.

Drawbacks:

- Time delay.
- More complex networks.

D. The Effect of Eavesdroppers on Network Connectivity: A Secrecy Graph Approach

Network connectivity is defined in a percolation sense, i.e., connectivity exists if an infinite connected component exists in the corresponding *secrecy graph*. We consider uncertainty in location of eavesdroppers, which is modeled directly at the *network level* as correlated failures in the secrecy graph. Our approach attempts to bridge the gap between physical layer security under uncertain channel state information and network level connectivity under secrecy constraints. Both analytic and simulation results show that uncertainty in location of eavesdroppers has a dramatic effect on network connectivity in a secrecy graph.

The percolation threshold is the critical value of probability of occurrence of an eavesdropper, above which an infinite connected component does not exist in the secrecy graph, almost surely. Hence, this paper provides bounds on percolation threshold for square and triangular lattices, which provide insight into the effect of uncertainty in eavesdropper's location on the percolation properties of lattice secrecy graphs.

Merit:

- Multiple data transmission

Drawback:

- Data loss in intermediate nodes

E. Towards Achieving Full Secrecy Rate in Wireless Networks A Control Theoretic Approach

We address two separate problems, both of which involve the maximization of a long-term average utility, defined as a function of the number of secure packets transmitted in each time slot. We propose a transmission controller and an admission controller based on simple index policies that do not rely on any prior statistical information on the data arrival process. The former chooses a random key generation (and transmission) rate as well as the secure data transmission rate in each time slot. Part of the data is secured by the available secrecy rate while the other part is encrypted by the key bits, enqueued at both the transmitter and the receiver. The latter chooses the amount of data admitted by the transmitter to be enqueued in the data queue. We show that our controller pair has a provably efficient performance.

This paper illustrate via simulations that the use of a key queue reduces the *queuing delay* for the data packets, while serving packets that are admitted at the maximum admissible rate. To our best knowledge, this is the first work that addresses the queuing delay in the context of secrecy.

Merit:

- Data is more secure

Drawback:

- Queuing delay in data path

III. PROPOSED SYSTEM

Our proposed system implements the wireless ad hoc network with 'n' number of nodes that should construct the network for data transmission from one location to another. Each node is having the unique id and its related locations. The randomly generated eavesdropping nodes are also present with in this network. The nodes are moving with static velocity and also the moving position of the each node is mentioned with (x, y) co-ordinates. Then the network should establish the connection with base station. Then the user should select the source, destination node and message and transmission range of the base station. If the distance between the source and destination is within the transmission range the direct data transmission is possible otherwise the transmission is relay transmission. ie. The message forwarded between the relay nodes, in which the relay nodes are either original nodes or eavesdroppers. In this situation we can analyze the security of the connection and overall efficiency of the network.

We consider a relay network consisting of one source (*S*), several relays (*Rl , l* = 1, 2, . . .), one destination (*D*), and several eavesdroppers (*E j , j* = 1, 2, . . .). All the nodes are equiped with one antenna. The distance between the source and destination is equal to d_{SD}. The distributions of relays and eavesdroppers are homogenous PPPs Φ_R and Φ_E with density $\lambda_R$and λ_E, respectively. In this system, all the transmitters transmit with the same power. Then we can obtain the instantaneous signal-to-noise ratio (SNR) at the relays, destination, and eavesdroppers as

$$SNR_{nm} = \varepsilon h_{nm} d_{nm}^{-\alpha}$$

Where,

ε → transmit SNR.

h_{nm} → small-scale fading (follows exponential distribution with unit mean)

$d_{mn} = ||x_m - x_n||$ → Euclidean distance between node *n* and node *m* mean.

x_n → location of node *n*.

α → path-loss exponent.

The relay transmission is not necessary if the direct transmission is strong enough. According to d_{SD}, we can know how strong the direct transmission is. For colluding eavesdroppers, to avoid relaying for the users having strong direct transmission we define a target secure connection probability δ constraint for direct transmission. Assume eavesdroppers cannot be allowed to collude and exchange information. The secure performance is determined with the strongest received signal from the transmitter

A. Distance between source, relay and destination

A relay network consisting of one source (S), several relays (R_l, l = 1, 2,), one Destination (D) and several eavesdroppers (E_j, j = 1, 2, . . .). All the nodes are equipped with one antenna. The distance between the source and destination is equal to d_{SD}. The source performs relay selection and decides whether a relay is needed. We assume that d_{SD}, and the node densities, a polar coordinate system is set up in which the source and destination locates at (d_{SD} /2, 0) and (d_{SD} /2, π), respectively. In a polar coordinate system, for a relay at xR_l= (r, θ), define two auxiliary functions to represent the distances from the arbitrary relay to the source and the destination respectively.

$$d_{SRl} = || x_S - x_{Rl} || = \sqrt{r^2 + (d^2_{SD} \div 4) - r d_{SD} \cos\theta}$$

$$d_{RlD} = || x_{Rl} - x_D || = \sqrt{r^2 + (d^2_{SD} \div 4) + r d_{SD} \cos\theta}$$

B. Secure Connection Probability

An arbitrary relay R_l, the message is secure only if both the $S \rightarrow R_l$link and the $R_l \rightarrow D$ link are secure. Thus, the secure connection probability can be obtained as follows.

$$P_{C\_Rl} = P\,(1/2 \log_2 [(1+\varepsilon h_{SRl} d_{SRl}^{-\alpha}) / (1+\varepsilon I_S)] > 0,\ 1/2 \log_2 [(1+\varepsilon h_{SRl} d_{RlD}^{-\alpha}) / (1+\varepsilon I_{Rl})] > 0)$$

$$P_{C\_Rl} = P\,([(h_{SRl} d_{SRl}^{-\alpha}) / (I_S)] > 1, [(h_{SRl} d_{RlD}^{-\alpha}) / (I_{Rl})] > 1)$$

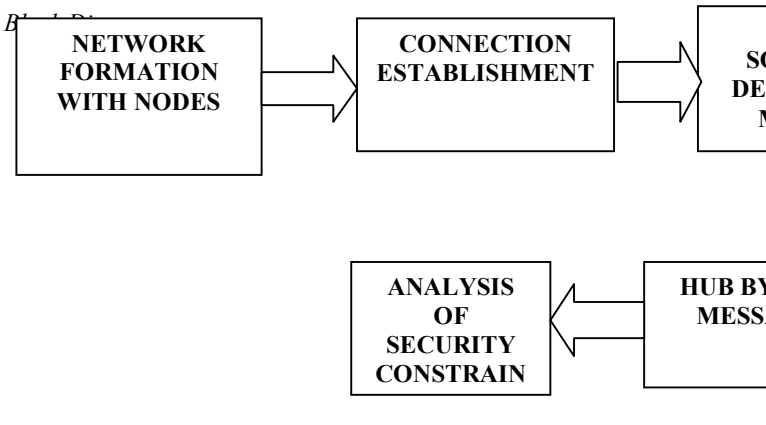
$$P_{C\_Rl} = E_{I_S, I_{Rl}}(\exp [- Is\, d_{S R l}^{\alpha} - I_{Rl} d_{R l D}^{\alpha}])$$

$$P_{C\_Rl} = L_{I_S, I_{Rl}} (d_{SRl}^{\alpha}, d_{R l D}^{\alpha})$$

Where $L_{I_S, I_{Rl}}(\cdot, \cdot)$ is the joint Laplace transform of $I_S$and I_{Rl}.

Then, the secure connection probability for an arbitrary relay can be written as, $P_{C\_Rl} = \exp[- (A\, d_{S R l}^2 + A\, d_{R l D}^2 - \lambda E f(d_{S R l}^{\alpha}, d_{R l D}^{\alpha}))]$

Block Diagram



C. Techniques
Dynamic Source Routing

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration. Network nodes cooperate to forward packets for each other to allow communication over multiple "hops" between nodes not directly within wireless transmission range of one another. As nodes in the network move about or join or leave the network, and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by the DSR routing protocol

Homogeneous Poisson Point Process

The homogeneous Poisson process is the simplest stochastic model for a planar point pattern. A realization of a homogeneous Poisson process is given in Figure.

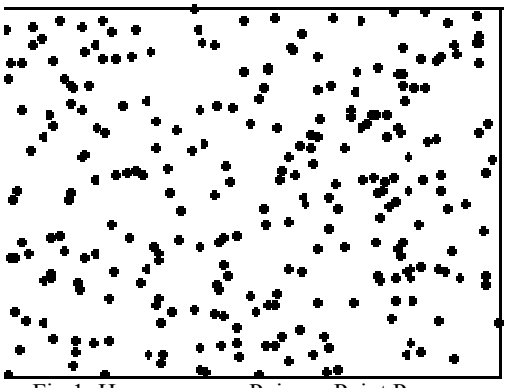


Fig 1: Homogeneous Poisson Point Process

The idea of this model is that the point events of interest occur completely independently of each other. This lack of interaction between points is called *complete spatial randomness.* We begin with the mathematical definition and some simple properties of homogeneous Poisson processes which can be introduced in a similar way as for the Poisson process on the real line via the counting variables X (B).

Let ν denote the (2-dimensional) Lebesgue measure in $\mathbf{R}^2$.Then, X is called a homogeneous Poisson process if there is a constant $\lambda>0$ such that 1) the number of points X (B) is Poisson distributed with parameter $\lambda> \nu(B)$, for each bounded Borel set B, and 2) the random variables $X(B_1),\ldots X(B_n)$ are independent for each finite sequence $B_1,\ldots,B_n$ of disjoint bounded Borel sets. Note that property (2) is the complete spatial randomness mentioned above. Furthermore, the parameter λ occurring in property (1) is the expected number of points per unit area, that is E $X(B)= \lambda\ \nu(B)$ for all bounded $B \in \beta$. Thus, λ is called the intensity of X. Another (so-called local) characterization of λ is connected with the fact that $\mathbf{P}(X(B)>0)= \lambda\ \nu(B)+o(\nu(B))$as $\nu(B)->0$. That is, for small sets B, the probability that there is at least one point in B is nearly proportional to λ.

IV. **RESULTS AND DISCUSSION**

The transmission of a confidential message from a source to a destination in a decentralized wireless network in the presence of randomly distributed eavesdroppers. Assuming that a relay at an arbitrary location is already chosen and it define the exact expression of secure connection probability for relay transmission. The source and the destination pair can be potentially assisted by randomly distributed relays. For an arbitrary relay, we derive exact expressions of secure connection probability for eavesdroppers. Comparison of the secure connection probability for direct transmission and relay transmission is also done. We address the important problem of whether or not to relay and discuss the condition for relay transmission in terms of the relay density and source, destination distance. These analytical results are accurate in the small eavesdropper density regime. The results obtained from this study provide useful design insights for relay networks with security constraints.

Fig2: Simulation result for Node Establishment

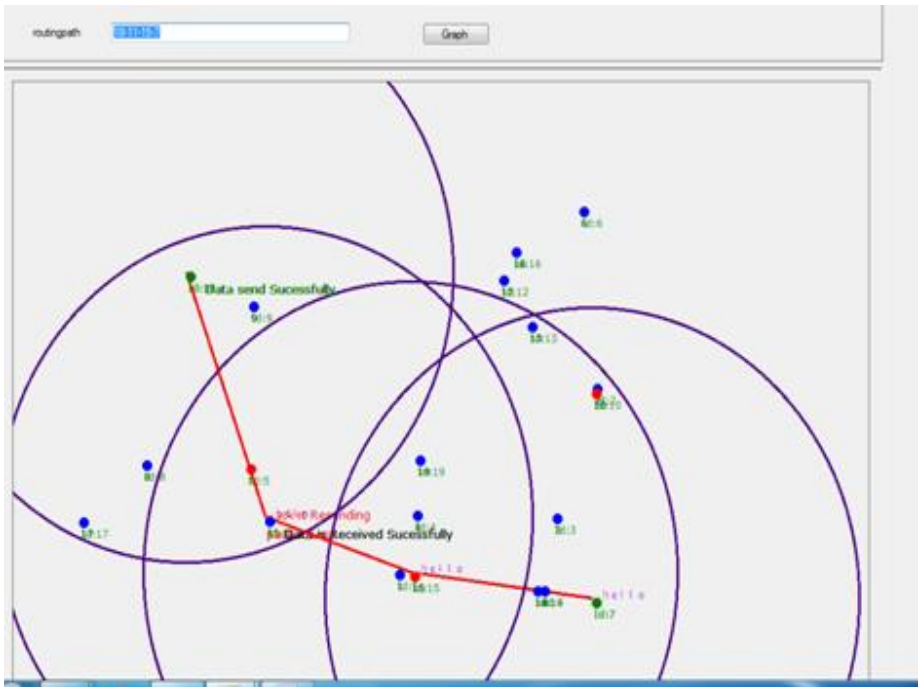


Fig 3: Simulation result for Hub By Hub Data Transmission.

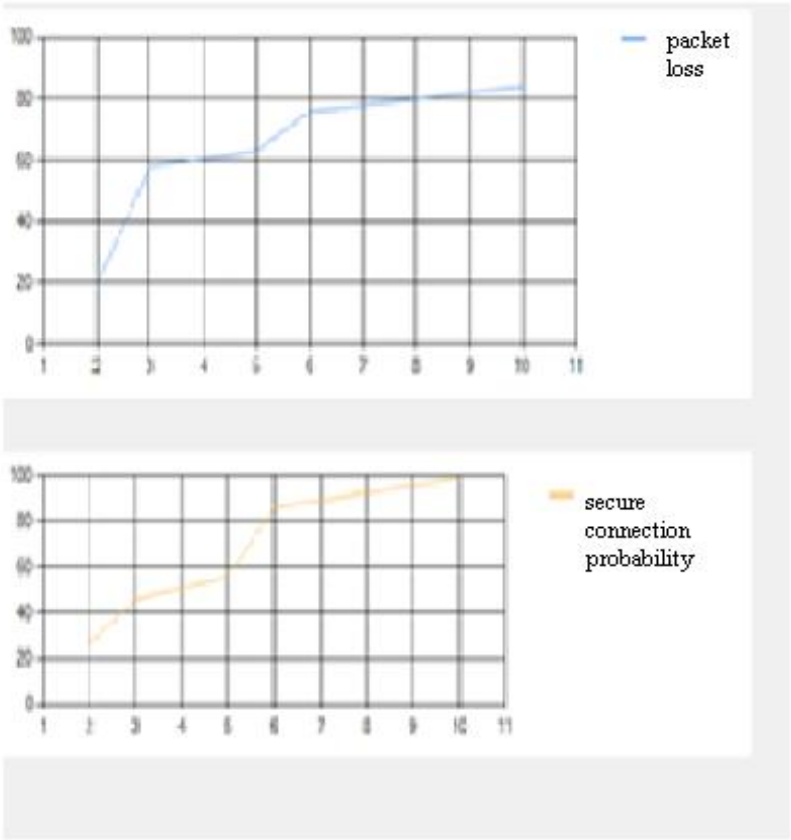


Fig 4: Simulation result for Comparision about Packet Loss with Number of Eavesdroppers and Secure Connection Probability with Number of Eavesdroppers.

V .CONCLUSION AND FUTURE WORK

I have analysed the secure connection probability of direct transmission and relay transmission for eavesdropper's strategies, where the distributions of relays and eavesdroppers follow homogenous Poison Point Process. Also analysed the problem of secure connectivity against eavesdroppers where the source-destination pair is assisted by a single randomize-and-forward (RAF) relay. The lower bound expressions of secure connection probability using RAF for eavesdropper's strategies are obtained, and it shows that the lower bound gives accurate approximation of the exact performance in the small eavesdropper density regime. Comparing the direct transmission with the relay transmission, we find that whether or not to relay transmission depends on the relay density and the distance between the source and destinations for a given target secure connection probability.

An interesting future work is to consider the confidentiality of the message should be transferred between the source and Destination of the Wireless Ad-hoc Network with Cryptographic Security mechanism using hash function. Hash function is used to encrypt the message at source node and forwarded through the arbitrary relay with the public key of source node then the encrypted message should automatically decrypted at relevant destination node with the help of receiver's private key and also is to consider multi-relay transmission and determine the condition under which relaying gives more secure connection.

ACKNOWLEDGEMENT

I would like to thank my guide Mr.P.BRIGHT PRABAHAR Asst. Prof., Electronics and communication engineering Department, Parisutham Institute of Technology and Science, Thanjavur for his help and guidance to enable us to propose this system.

REFERENCES

[1] D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8,pp. 1355–1387, Oct. 1975.
[2] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wirelessinformation-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6,pp. 2515–2534, Jun. 2008.

[3] M. Haenggi, "The secrecy graph and some of its properties," in Proc.IEEE Int. Symp. Information Theory, Toronto, ON, Canada, Jul. 2008.
[4] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication instochastic wireless networks—Part I: Connectivity," IEEE Trans. Inf.Forensics Security, vol. 7, no. 1, pp. 125–138, Feb. 2012.
[5] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, " Modelinglocation uncertainty foreavesdroppers: A secrecy graph approach,"in Proc. IEEE ISIT, Austin, TX, USA, Jun. 2010, pp. 2627–2631.
[6] P. C. Pinto and M. Z. Win, "Continuum percolation in the intrinsicallysecure communications graph," inProc. ISITA, Taichung, Taiwan, Oct.2010.
[7] X. Zhou, R. Ganti, and J. Andrews, "Secure wireless network connec-tivity with multi-antenna transmission,"IEEE Trans. Wireless Commun.,vol. 10, no. 2, pp. 425–430, Feb. 2011.
[8] L. Lai and H. El Gamal, "The relay–eavesdropper channel: Cooperationfor secrecy," IEEE Trans. Inf. Theory, vol. 54, no. 9, pp. 4005–4019,Sep. 2008
[9] .Jeong and I.-M. Kim, "Optimal power allocation for secure multi-carrier relay systems," IEEE Trans. Signal Process., vol. 59, no. 11,pp. 5428–5442, Nov. 2011.
[10] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wirelessphysical layer security via cooperating relays," IEEE Trans. SignalProcess., vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

BIOGRAPHY

R.VENKATESHARJUN[1] received degree B.E (ECE) from AnjalaiAmmalMahalingam Engineering College, Tiruvarur, Tamilnadu, India, affiliated to Anna University Chennai in 2012. He is currently persuading M.E – Communication Systems in Parisutham Institute of Technology and Science, Thanjavur, Tamilnadu, India