International Journal of Electrical Electronics Computers & Mechanical Engineering (IJEECM)
ISSN: 2278-2808
www.ijeecm.org Volume 8 Issue 5 ǁ July. 2018

IJEECM journal of Computer Science Engineering (ijeecm-jcs)

Secure Relay Data communication in untrusted cooperative Networks

M Vikas[1], N V Ashok kumar[2], Dr. C P V N J MohanRao[3]

[1,2,3] *Computer Science Engineering Department,*

[1,2,3] Avanthi Institute of Engg & Technology, Narsipatnam, Visakhapatnam (Dt), A.P., India

Abstract: **This project studies the problem of secure transmission in dual-hop cooperative networks with untrusted relays, where each relay acts as both a potential helper and an eavesdropper. A security-aware relaying scheme is proposed, which employs the alternate jamming and secrecy-enhanced relay selection to prevent the confidential message from being eavesdropped by the untrusted relays. To evaluate the performance of the proposed strategies, we derive the lower bound of the achievable ergodic secrecy rate (ESR), and conduct the asymptotic analysis to examine how the ESR scales as the number of relays increases.**

Index Terms— Secure routing; Manets; Graph; QoS; Attacks.

I. INTRODUCTION

Cooperation is the process of working together, opposite of working separately in competition. Recently, such a concept has been adopted from social sciences and economics to constitute a major research area in wireless communication networks. The idea of employing cooperation in wireless communication networks has emerged in response to the user mobility support and limited energy and radio spectrum resources, which pose challenges in the development of wireless communication networks and services in terms of capacity and performance. Generally, we can categorize three cooperation scenarios based on various studies in literature. In the first scenario, cooperation among different entities is employed to improve the wireless communication channel reliability through spatial diversity [1], [2]. In the second scenario, the system throughput is improved via aggregating the offered resources from cooperating entities [3], [4]. Finally, cooperation is used to achieve seamless service provision [5] - [8]. Early research on cooperation in wireless communication networks focuses on developing strategies at the physical layer to support such a cooperative transmission. However, such a cooperative operation introduces challenging issues at different layers of the network protocol stack. Some modifications to the networking protocol stack are required to achieve the objectives of coop-eration. In fact, without proper modification of networking protocols at the higher layers, the achieved cooperation gain may not be significant.

II. IMPROVED CHANNEL RELIABILITY

A. Mitigating Channel Impairments:

The wireless communication channel suffers from several phenomena that decrease its re-liability. These phenomena include path loss, shadowing, and fading. Cooperation in wireless networks can increase the reliability of the communications against the channel impairments. This improved reliability can be achieved by exploiting cooperative spatial diversity [1], [2]. When the channel between the original source and destination is unreliable, other network entities can cooperate with the source node to create a virtual antenna array and forward the data towards the destination. Hence, different transmission paths with independent channel coefficients exist between the source and destination nodes through the cooperating entities. As a result, the destination node receives several copies of the transmitted signal over independent channels. Based on this spatial diversity, the destination can combine the data received from these entities in detection to improve the transmission accuracy. This concept is illustrated in Figure 1(a) for a downlink transmission from a base station to a mobile terminal, where the source node transmits its data packets towards the destination node with the help of cooperating entities. In this context, a cooperating entity is a relay node with an improved channel condition over the direct transmission channel from the source to the destination. This relay node can be a mobile terminal or a dedicated relay station

B. Interference Reduction:

The broadcast nature of the wireless communication medium results in interference at the different nodes in the coverage area (interference region) of each other. Such interference reduces the signal to interference plus noise

ratio (SINR) at the receiving nodes and hence degrades their detection performance. Thanks to the cooperation introduced by the cooperative relays, the transmitted power from the original source can be significan tly reduced due to a better channel condition of the relaying links, which greatly reduces the interference region [9], as illustrated in Figure 1(b). This also helps to improve the energy efficien cy of the communication system. In addition to reducing the interference region, cooperation can solve the hidden terminal problem and hence results in interference reduction [10].

III. IMPROVED SYSTEM THROUGHPUT

An improved system throughput can be a direct benefit from the enhanced wireless channel reliability through employing cooperative transmissions at the physical layer. In addition, co-operation can increase the achieved throughput through aggregating the offered resources from different cooperating entities [3], [4]. This is achieved through employing cooperative strategies at the network and transport layers. In this case, data packets are transmitted along multiple paths towards the destination. Different from the preceding cooperation scenario, the data packets transmitted through different paths are not the same copy of some transmitted signal. Instead, different transmission paths carry different data packets. This has the effect of increasing the total transmission data rate between the source and destination nodes. In this case, the cooperating entities can be mobile terminals, base stations or access points with sufficient resources (e.g. bandwidth), such that when these resources are aggregated, the total transmission data rate from the source to the destination can be increased. This strategy can support applications with a high required transmission rate. In Figure 2 for example, resources from the cooperating cellular network and wireless local area network (WLAN) are aggregated to provide a high data rate for the mobile terminal.

IV. PROBLEM STATEMENT/SPECIFICATION

In untrusted relay systems have been reported, the majority of existing works deal with the simple model with only one relay node. For multi-relay networks, information leakage problem during the first phase of any two-hop transmission. This simplifies the protocol design, but may not hold in practice. So secure the transmissions of both the first and the second phases is the major problem which needed to be solved

1) Diverse results on untrusted relay systems have been reported, the majority of existing works deal with the simple model with only one relay node.

2) Information leakage problem during the first phase of any two-hop transmission.

3). No cooperative scheme considers relay as an outside entity, which does not take part in communication, hence it is considered as an eavesdropper

4) Relays may have poor security authorization

V. PROPOSED SYSTEM

In this project try to secure, the transmissions of both the first and the second phases, and our contributions are threefold: First, an alternate jamming method is introduced to prevent information leakage. Second, both optimal and sub-optimal secrecy-enhanced relay selection policies are proposed third, the lower bound of the achievable ergodic secrecy rate (ESR) is derived, and the asymptotic analysis of the ESR is given as well.

A. Advantages of proposed System:-

we first consider a two hop system where the direct link is not available between the source node and the destination node, Achievable secrecy rates at different positions of the jammer.

An AF based network consisting of a source (S), a destination (D), an untrusted relay (R) and a cooperative jammer (CJ) which assists in jamming the signal at the relay by transmitting a noise signal that is known at the destination.

the secrecy rate regions for different scenarios depends heavily on the positions of both the relay (a potential eavesdropper) and the cooperative jammer

Higher Spatial Diversity

Higher Throughput-Lower Delay

VI. ITERATIVE BOOSTING ALGORITHM

relay path reconstructs unknown long paths from known short paths iteratively. By comparing the recorded hash value and the calculated hash value, the sink can verify whether a long path and a short path share the same path after the short path's original node. When the sink finds a match, the long path can be reconstructed by combining its original node and the short path.

Initial set of packets whose paths are reconstructed and a set of other packets are considered.

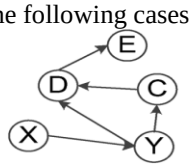
Checking the value of initial path. If value is null, then it is network failure else it constructs another path with another packet.

This process is repeated till the paths are their weights are obtained in the network.

The shortest path is considered and it is compared with remaining paths and the values are stored in the database.

The algorithm consists of two processes, the Iterative-Boosting procedure and the **Recover** procedure. The Iterative-Boosting procedure includes the main logic of the algorithm that tries to reconstruct as many as possible packets iteratively. The input is an initial set of packets whose paths have been reconstructed and a set of other

packets. During each iteration, is a set of newly reconstructed packet path the algorithm tries to use each packet in to reconstruct each packet's path. The procedure ends when no new paths can be reconstructed. The **Recover** procedure tries to reconstruct a long path with the help of a short path. Based on the high path similarity observation, the following cases describe how to reconstruct a long path.



$path(c_1) = (C, D, E)$ (known)

$path(y_1) = (Y, C, D, E)$ (unknown)
$path(x_1) = (X, Y, C, D, E)$ (unknown)
$path(x_2) = (X, Y, D, E)$ (unknown)

Case 1: $hash(Y, path(c_1)) = h(y_1) \rightarrow path(y_1) = (Y, C, D, E)$

Case 2: $hash(X, Y, path(c_1)) = h(x_1) \rightarrow path(x_1) = (X, Y, C, D, E)$

Case 3: $hash(X, Y, path(c_1) - C) = h(y_2) \rightarrow path(y_2) = (X, Y, D, E)$

VII. FAST BOOTSTRAPPING ALGORITHM

The iterative boosting algorithm needs an initial set of reconstructed paths. In addition to the one/two-hop paths, the fast bootstrapping algorithm further provides more initial reconstructed paths for the iterative boosting algorithm. These initial reconstructed paths reduce the number of iterations needed and speed up the iterative boosting algorithm. The fast bootstrapping algorithm needs two additional data fields in each packet, parent change counter and global packet generation time. The parent change counter records the accumulated number of parent changes, and the global packet generation time can be estimated by attaching an accumulated delay in each packet. For packet , there are an upper bound and a lower bound of the difference between the estimated packet generation time and the real value .The basic idea is to reconstruct a packet's path by the help of the local packets at each hop. For each node, we can obtain its **stable periods** by the parent change counter attached in each of its local packet. A stable period of a node is a period of time in which the node does not change its parent. If a packet is forwarded by this node in one of its **stable periods,** we can safely reconstruct the next-hop of that forwarded packet to be the parent of its local packet in the same stable period.

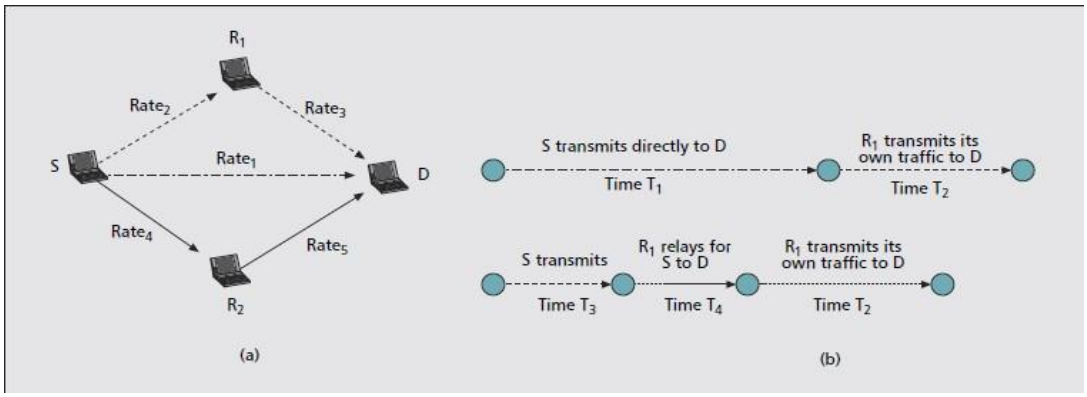


Fig 1:a) Cooperation in a network; b) illustration of the delay and throughput improvement achieved by cooperation in the time domain

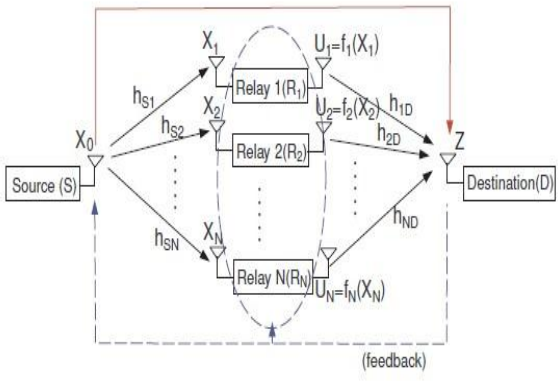


Fig 2 dual hop network model

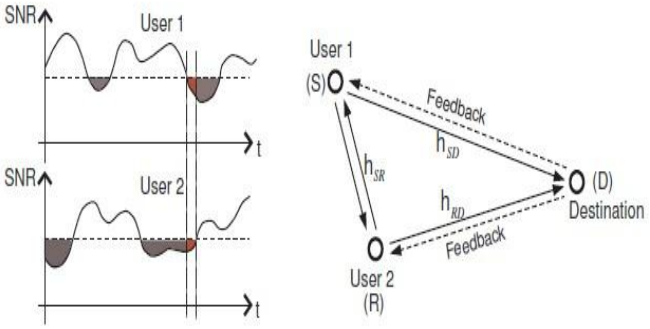


Fig 3: A three-node cooperative network model Decode and Forward Method

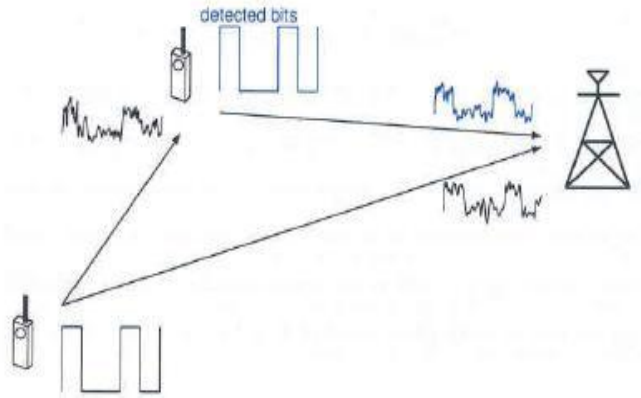


Fig 4:- This will decode the message received from the source, re-encodes it and then forwards the message to the destination subsequently

Amplify and Forward Method

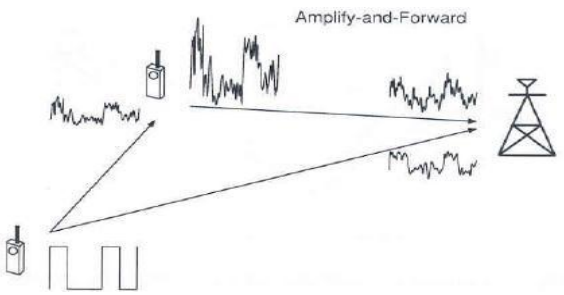


Fig 5 The relay node simply amplifies the received signal and forwards it directly to the destination without decoding the message.

VIII. EXPERIMENTAL/SETUP AND RESULTS

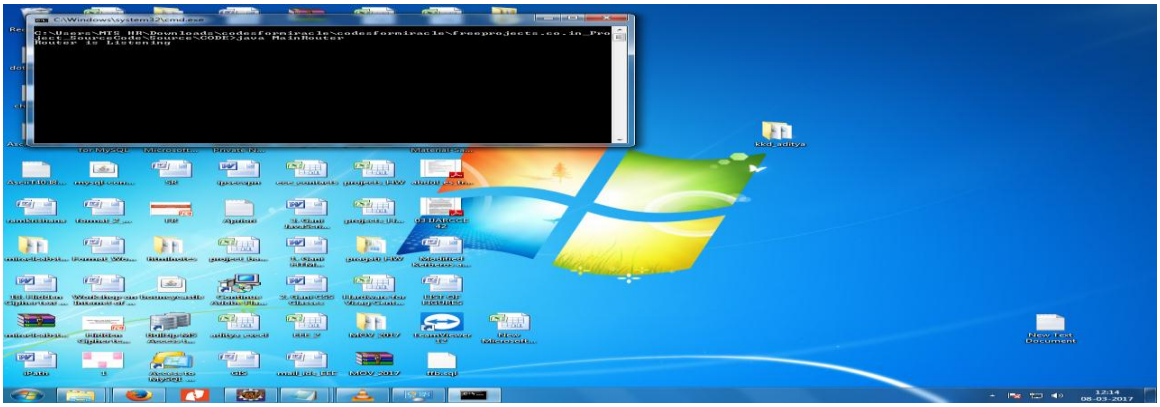


Fig 6 : Creating the network with required number of nodes

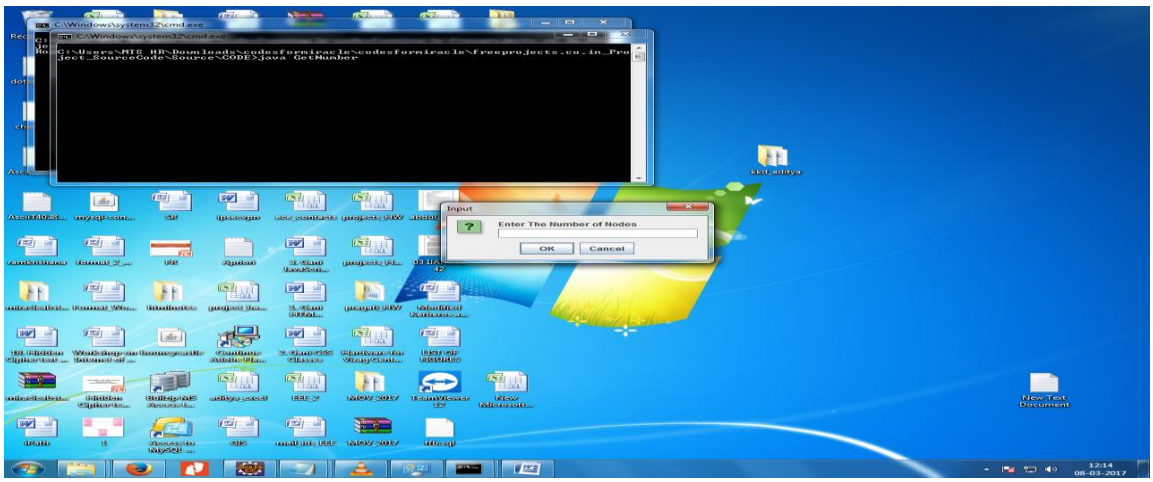


Fig 7 Node registration

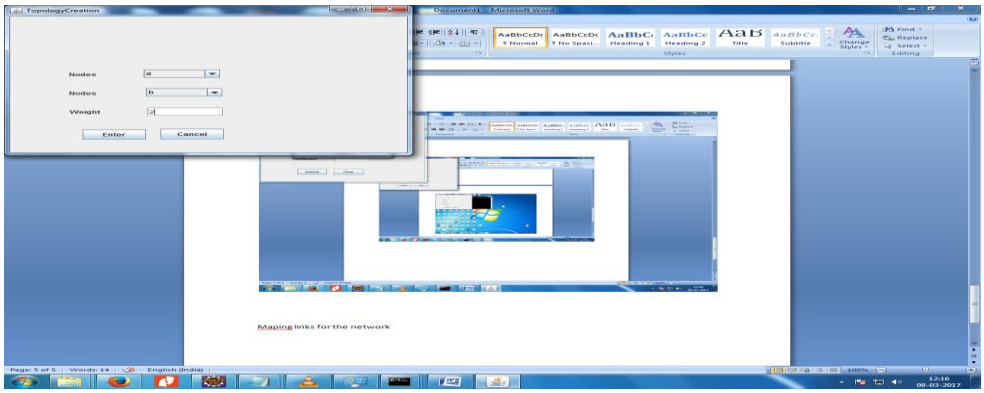


Figure 8 Path consturction

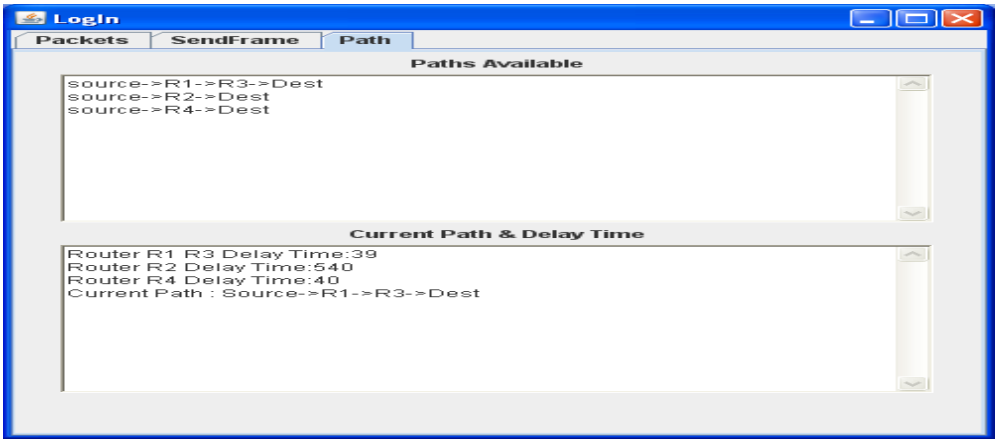


Figure 9 Selected Router Process

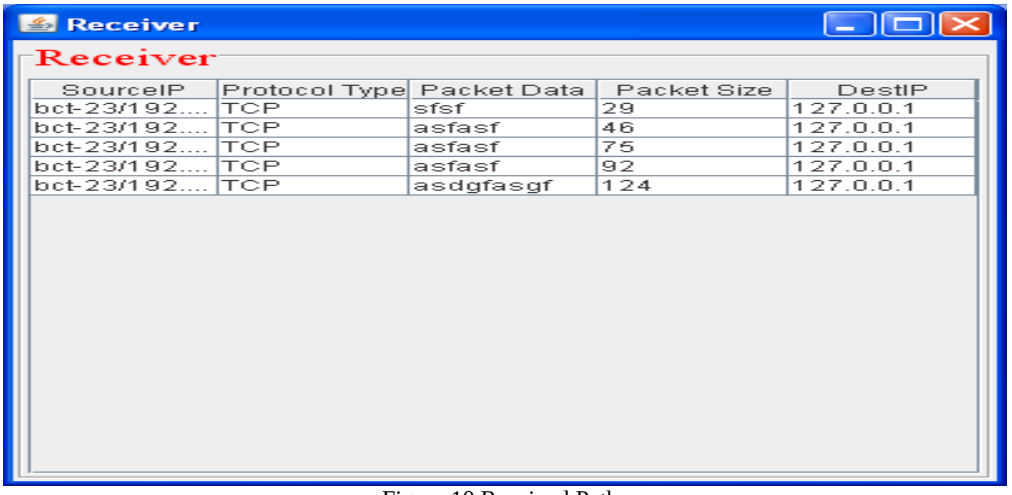


Figure 10 Received Paths

IX. CONCLUSION

In this paper, we have investigated the secrecy regions for friendly jamming in two-hop as well as the cooperative scenarios employing an untrusted relay. Our results show that the secrecy rate regions for different scenarios depends heavily on the positions of both the relay (a potential eavesdropper) and the cooperative jammer. We show that the secrecy rates are higher if the jammer is positioned closer to the relay. If the relay is closer to the destination then we can ensure a higher secrecy rate in comparison to the case when the relay is closer to the source

REFERENCES

[1]. K. Ingols, R. Lippmann, and K. Piwowarski, “Practical attack graph generation for network defense,” in Computer Security Applications Conference, 2006., 12 2006, pp. 121 –130.

[2]. S. Jajodia, S. Noel, and B. O’Berry, “Topological analysis of network attack vulnerability,” in Managing Cyber Threats: Issues, Approaches and Challanges, V. Kumar, J. Srivastava, and A. Lazarevic, Eds. Kluwer Academic Publisher, 2003, ch. 5.

[3]. L. H. G. Ferraz, P. B. Velloso, and O. C. M. B. Duarte, "An Accurate and Precise Malicious Node Exclusion Mechanism For Ad Hoc Networks," Ad Hoc Networks - Elsevier B.V., vol. 19, pp. 142–155, 2014.

C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc on-demand distance vector (AODV) routing," 2070-1721, 2003.

[4]. J. Mo, M. Tao, Y. Liu, and R. Wang, “Secure beamforming for mimo two-way communications with an untrusted relay,” IEEE Trans. Signal Process., vol. 62, no. 9, pp. 2185–2199, May 2014.

[5]. Y. Zou, X. Wang, and W. Shen, “Optimal relay selection for physicallayer security in cooperative wireless networks,” IEEE J. Sel. Areas Commun., vol. 31, no. 10, pp. 2099–2111, Oct. 2013.

[6]. 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 J. Sel. Areas Commun., vol. 29, no. 10, pp. 2067–2076, Dec. 2011.

[7]. A. Sheikholeslami, M. Ghaderi, H. Pishro-Nik, and D. Goeckel, “Jamming-aware minimum energy routing in wireless networks,” in Proc. IEEE Int. Conf. Commun. (ICC), June 2014, pp. 2313–2318.

[8]. Z. Ding, K. Leung, D. Goeckel, and D. Towsley, “On the application of cooperative transmission to secrecy communications,” IEEE J. Sel. Areas Commun., vol. 30, no. 2, pp. 359–368, Feb. 2012.

[9]. X. Zhou, R. Ganti, J. Andrews, and A. Hjorungnes, “On the throughput cost of physical layer security in decentralized wireless networks,” IEEE Trans. Wireless Commun., vol. 10, no. 8, pp. 2764–2775, Aug. 2011.

[10]. M. Saad, “Joint optimal routing and power allocation for spectral efficiency in multi-hop wireless networks,” IEEE Trans. Wireless Commun., vol. 13, no. 5, pp. 2530–2539, May 2014.

[11]. C. Wang, H.-M.Wang, and X.-G. Xia, “Hybrid opportunistic relaying and jamming with power allocation for secure cooperative networks,” IEEE Trans. Wireless Commun., vol. 14, no. 2, pp. 589–605, Feb 2015.

[12]. J. Li, A. Petropulu, and S. Weber, “On cooperative relaying schemes for wireless physical layer security,” IEEE Trans. Signal Process., vol. 59, no. 10, pp. 4985–4997, Oct. 2011.

[13]. C. Ma, J. Liu, X. Tian, H. Yu, Y. Cui, and X. Wang, “Interference exploitation in d2d-enabled cellular networks: A secrecy perspective,” IEEE Trans. Commun., vol. 63, no. 1, pp. 229–242, Jan. 2015.

[14]. H. Wang, X. Zhou, and M. Reed, “Physical layer security in cellular networks: A stochastic geometry approach,” IEEE Trans. Wireless Commun., vol. 12, no. 6, pp. 2776–2787, May 2013.

[15]. C. Cai, Y. Cai, X. Zhou, W. Yang, and W. Yang, “When does relay transmission give a more secure connection in wireless ad hoc networks?” IEEE Trans. Inf. Foren. Sec., vol. 9, no. 4, pp. 624–632, Apr. 2014

[16]. D. Wang and P. Wang, "Understanding Security Failures of Two-Factor Authentication Schemes For Real-Time Applications In Hierarchical Wireless Sensor Networks," Ad Hoc Networks - Elsevier B.V., vol. 20 pp. 1–15, 2014.

Author’s Profile:

M Vikas completed B.Tech IT(Information technology) from Avanthi institute of engineering and technology under jntuk. M.Tech computer science and engineering from Avanthi institute of engineering and technology under jntuk , Visakhapatnam, Andhra Pradesh

N V Ashok Kumar. M.Tech (CSE) He received the B.Tech degree in Computer Science and Engineering from JNT University, Kukatpalli, Hyderabad and received the M.Tech degree in Computer Science and Technology from JNT University, Kakinada. Presently he is working as Assistant Professor in Computer Science and Engineering in Avanthi Institute of Engineering and Technology,Vizag, A.P.His research interests include Network Security, Data Warehousing and Data Mining and RDBMS .He has Published more than 10 papers in various national and international journals.

Dr. C P V N J MohanRao is Professor in the Department of Computer Science and Engineering, Avanthi Institute of Engineering & Technology - Narsipatnam. He did his PhD from Andhra University and his research interests include Image Processing, Networks, Information security, Data Mining and Software Engineering. He has guided more than 50 M.Tech Projects