Advances in Modelling and Analysis D
Vol. 23, No. 1, December, 2018, pp. 6-11
Journal homepage: http://iieta.org/Journals/AMA/AMA_D

Secured communications in cognitive radio networks

T. Perarasi*, G. Nagarajan

Department of ECE, Pondicherry Engineering College, Puducherry 605 104, India

Corresponding Author Email: appu_pera@yahoo.com

https://doi.org/10.18280/ama_d.230102

Received: 22 March 2018
Accepted: 15 June 2018

Keywords:
attacks, differential key pre-distribution, EGPSR,GPSR, hop by hop communication, routing protocol

ABSTRACT

Enabling end to end secure communications between source and sink is significant for many Cognitive Radio Networks (CRNs). While there have been many works devoted to hop by hop secure communications, the issue of end to end secure communications is largely ignored. In this paper, an end to end secure communication protocol in randomly deployed CRNs is designed. Specifically; this protocol is based on a methodology called differentiated key pre-distribution. The core idea is to distribute different number of keys to different nodes to enhance the resilience of certain links. This feature is leveraged during routing, where users route through those links with higher resilience. Using rigorous theoretical analysis, an expression for the quality of end to end secure communications is derived and uses it to determine optimum protocol parameters. Extensive performance evaluation illustrates that the proposed solution can provide highly secure communications between relays and sink in randomly deployed CRNs.

1. INTRODUCTION

The basic random key pre distribution is a well-accepted scheme for secure communications in randomly deployed CRNs [1-2]. At the key pre-distribution stage, each user is pre distributed with k distinct keys randomly chosen from a large pool of K keys and then nodes are randomly deployed. At the pair wise key establishment stage, each user first obtains its neighborhood information. If two neighbors share one or more pre-distributed keys, they establish a pair wise key in between directly. To do so, one node can generate a random pair wise key and send it to its neighbor encrypted with their shared keys [3].

For two neighbors that do not share pre-distributed key, they will use neighboring nodes, called proxies, to construct key paths for pair wise key establishment. Many variants have been proposed based on the above idea of key pre-distribution in CRNs. While some works focus primarily on extensions to the basic scheme, other works focus on more involved extensions. There are also works that address end-to-end secure communications in radio networks without random key pre distribution techniques. One particularly interesting work is that primarily focuses on end-to-end data confidentiality by performing intermediate data aggregation via homomorphic encryption techniques. In their technique, each node can derive its own private key based on a master secret, which is only known to the user. Then, all data from sensors is encrypted with keys of other sensors via a homomorphic encryption technique that allows aggregation on encrypted data hop by hop, which can then be recovered by the user [4-6].

The downside of such attempts is that while in-network aggregation is done, in-network processing of data cannot be directly accomplished. Though there are several advantages with in-network processing of data like in network aggregation, localized verification of data trust and integrity, local filtering of malicious data etc. Furthermore, in applications where the user needs to know individual data, the work has limited applicability. The proposed work is different in the sense that end-to-end secure communications are focused via a combination of key management and routing techniques in the network, while still retaining the advantages of in-network aggregation [7-8].

An energy-efficient probabilistic group-based key distribution scheme for a large-scale heterogeneous wireless sensor network is proposed in [9]. This scheme always guarantees that any two non-compromised nodes in a deployment group can communicate each other with 100% secrecy. Moreover, it provides significantly better security against cognitive node captured as compared to that for the existing related schemes. Overall, the scheme has a better trade-off among network connectivity, security, communication and computational overheads than the existing related schemes.

Key establishment in sensor networks becomes a challenging problem because of the resource limitations of the sensors and also due to vulnerability to physical capture of the sensor nodes. An unconditionally secure probabilistic group-based key pre-distribution scheme for a heterogeneous wireless sensor network is considered. The proposed scheme always guarantees that no matter how many sensor nodes are compromised, the non compromised nodes can still communicate with 100% secrecy, i.e., the proposed scheme is always unconditionally secure against node capture attacks. Moreover, it provides significantly better trade-off between communication overhead, computational overhead, network connectivity and security against node capture as compared to the existing key pre-distribution schemes [10-11].

The schemes are analyzed in detail with respect to security and performance. Performance analysis shows that Tree-Based Scheme exhibits better performance which achieves rekey operation by performing log m and communications with some additional storage. In CRT Based Scheme, key is established in an efficient way for node addition, node compromise and also at regular intervals. The communication cost incurred at each node for establishing key is one receive operation and computation cost incurred is one modulus operation and one EX-OR operation by each node [11-12]. A deployment conscious security framework supporting, a shift of complex operations to more capable nodes of heterogeneous environment and relieving resource constrained generic sensor nodes of major activities is introduced in [13-15]. Through this work, it is able to conclude that a hybrid of asymmetric and symmetric key cryptography best suits heterogeneous environments. It can achieve quick authenticity without extra computations and communications.

Traditional key management techniques, such as public key cryptography or key distribution center (e.g., Kerberos), are often not effective for wireless sensor networks for the serious limitations in terms of computational power, energy supply, network bandwidth [16-17]. In contrast to other LEACH security solutions, the salient advantage of this work is the addressed challenging security issues of runtime phase by real time rekey, which can efficiently protect the network against attacks of eavesdropping or captured nodes compromise and so on are explained in [18]. Power allocation to the users and node are made based on the scheduling mechanism and handoffs between them are maintained. Tradeoff between the users are clearly projected and explained in [19-22].

2. EXISTING SYSTEM

There are two standard metrics namely Connectivity and Resilience. Connectivity is the probability that two physical neighbors can establish a pair wise key between them. Global (end to-end) connectivity is the probability that the entire network is securely connected, or as the number of nodes in the largest connected component of the secure network. Global connectivity can be inferred by local connectivity that focus only on local connectivity [23-24]. Resilience is the probability that a pair wise key between two nodes is not compromised under attack.

2.1 Routing protocols in WSNS

There are two main paradigms of routing protocols in CRNs namely; Location-centric routing and Data-centric routing.

Greedy Perimeter Stateless Routing (GPSR) is a well-known location centric routing protocol. In GPSR, beacon messages are broadcast by each node to inform its neighbors of its position. GPSR assumes that nodes can determine through separate means the location of the user. Each node makes forwarding decisions based on the relative position of the user and its neighbors. In general, the neighbor that is closest to the user is chosen [8]. Directed diffusion is the most renowned data centric routing protocol, in which the user sends queries to all nodes and waits for data from the nodes satisfying specific requirement. The interest is broadcast through the network and used by each node to compare with the data received. The interest entry also contains several gradient fields. A gradient is a reply link to a neighbor from which the interest was received. By utilizing interests and gradients, paths are established between sensors and the sink. Several paths may be established and one of them is selected by reinforcement.

2.2 Security protocol

End to end secure communication Protocol consists of two components like differentiated key management and resilience aware routing. The differentiated key management consists of two stages like Key pre distribution and Pair wise key establishment [23].

Table 1. Increase of the number of links with different number of shared keys under differentiated key pre-distribution

# of shared keys	0	1	2	3	4	5	6	7	8	>8
# of links increase	54%	8%	20%	29%	19%	2%	25%	56%	83%	75%

2.3 Key pre-distribution

A network with N users and one node are considered. The nodes are divided into c classes, each of which has ni ($1 \leq i \leq c$) nodes. Let the nodes in the it class as class i nodes. Pre-distribute ki ($1 \leq i \leq c$ and $k1 \geq k2 \geq \cdot\cdot\cdot \geq kc$) unique keys chosen from a large key pool with size K into each class i node, detail of which will be discussed in the following. It is to be noted that, the sink node is pre-distributed with all K keys in the key pool. After this, the user is deployed strategically at certain position, while the N nodes are deployed randomly in the network. The N nodes will execute the following protocols for pair wise key establishment and routing.

2.4 Pairwise key establishment

Once nodes are pre distributed with keys and deployed, they start to discover their neighbors within their communication range r via local communication and obtain the key IDs of their neighbors' pre-distributed keys. With the above information, each node constructs all the one-hop and two-hop key paths to all its neighbors. If node i shares pre-distributed keys with a neighbor j, there is one direct key path with one hop between them. However, node i will also construct all the two-hop key paths with each of its neighbors, regardless of whether a one-hop key path has been constructed or not, to enhance the link resilience. Suppose node i wants to construct all two-hop key paths with node j now. To do so, node i sends a request to its neighbors, containing the node IDs of i and j. After a neighboring node m receives the request, it checks if it shares pre-distributed keys with node i and shares pre-distributed keys with node j. If both conditions are satisfied, node m sends a reply back to node i. In this way, a two-hop key path i–m–j is constructed. If possible, other two-hop key paths are also constructed as above. After node i constructs all two hop key paths to node j, node i will generate multiple random key shares and transmit each key share on each key path. Key shares are encrypted/decrypted hop by hop by a combination of all shared keys on that hop [3].

Protections keys between i and j ((i, j)) is,

$$key(i, j) = k(i, j) + \sum_{l=1}^{p} \min(k(i, s_l), k(s_l, j)) \tag{1}$$

(i, j) may be calculated like this because the resilience of a two hop key path is mainly decided by the weaker link. The larger the number of protection keys for a link, the more resilient is the link in general.

Table 2. Protocol parameters

Notation	Protocol parameter
S	network area (= *πR*2)
R	communication range
N	number of nodes in the network
C	number of node classes
Ni	number of class *i* nodes (1 ≤ *i* ≤ *c*)
Ki	number of keys pre-distributed in class *i* node (1 ≤ *i* ≤ *c*)
K	number of keys in key pool
N_c	number of captured nodes

2.5 Location centric routing protocol

The location centric routing protocol is GPSR. In GPSR, each node chooses a neighbor as the next hop that is closest to the sink. In order to achieve high end to end secure communications without compromising network lifetime, extension of GPSR protocol are as follows. Each node i assigns a weight to all its secure neighbors that are closer to the user than itself. We denote $U(i)$ as the set of node i's secure neighbors that are closer to the user than itself and recall $key(i,j)$ is the number of protection keys for the link between nodes i and j, weight to each node j in set $U(i)$ is assigned as,

$$w_j = \frac{key(i, j)^{\alpha}}{\sum_{m \in U(i)} key(i, m)^{\alpha}} \qquad (2)$$

In traditional minimum hop routing protocol, a variant of Directed Diffusion routing protocol, a node will choose a neighbor on the minimum hop path to the user. This protocol can be extended in a similar way as above. During the next hop determination process, packets are forwarded only on the minimum hop secure paths. A secure path consists of links that have pair wise keys established. The set of neighbors on the minimum hop secure path of node i be (i). It is to be noted that in a relatively dense network; there could be several minimum hop secure paths between node i and the user as given in Figure 1. Node i then assigns a weight w_j to each of its secure neighbor's j in the set (i).

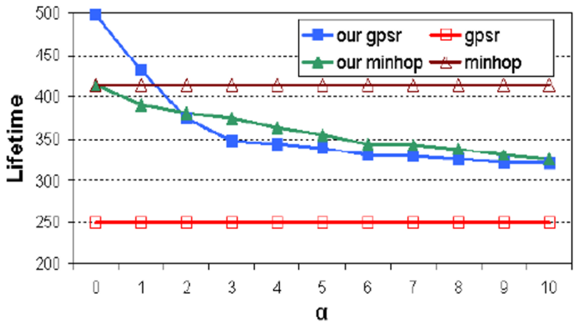

Figure 1. Sensitivity of lifetime to parameter *α*

2.6 Biased node capturing attack

Biased node capturing attack is one in which the attacker attempts to capture some special nodes in the network. Typically, the capture of those nodes results in higher attack impact and they are chosen with bias instead of randomly. The existence of such special nodes comes from the fact that the roles of sensor nodes in the network are inherently different. In a multi-hop network, the nodes near the user are such special nodes, whose capture results in more secret information disclosed to the attacker [24].

3. PROPOSED METHOD

Routing in sensor networks is very challenging due to several characteristics that distinguish them from contemporary communication and wireless ad-hoc networks. First of all, it is not possible to build a global addressing scheme for the deployment of sheer number of nodes. Therefore, traditional IP based protocols cannot be applied to radio networks. Second, in contrary to typical communication networks almost all applications of radio networks require the flow of sensed data from multiple sources to a particular user. Third, generated data traffic has significant redundancy in it since multiple nodes may generate same data within the vicinity of a phenomenon. Such redundancy needs to be exploited by routing protocols to improve energy and bandwidth utilization. Fourth, nodes are tightly constrained in terms of transmission power, on-board energy, processing capacity and storage and thus require careful resource management.

3.1 Greedy perimeter stateless routing (GPSR)

GPSR supports two mechanisms for forwarding data packets. They are Greedy forwarding and Perimeter forwarding. In Greedy Forwarding**,** all data packets are forwarded to an adjacent neighbor that is geographically positioned closer to the intended destination. This mechanism is known as greedy forwarding. In perimeter mode, the data packet is marked as being in perimeter mode along with the location where greedy forwarding failed. These perimeter mode packets are forwarded using simple planar graph traversal. Each node receiving a data packet marked as in perimeter mode uses the right hand rule to forward packets to nodes, which are located counterclockwise to the line joining forwarding node and the destination.

GPSR scans its neighborhood table to retrieve the next hop which is optimal and leads to the destination, during packet transmission to a known host. As there may be more than one such hop available, GPSR selects an adjacent neighbor that has the least distance to a particular destination. In S-GPSR, the trust levels used in conjunction with the geographical distances are incorporated in the neighborhood table to create the most trusted distance route rather than the default minimal distance to compute direct trust in a node, an effort-return based trust model is used. The accuracy and sincerity of immediate neighboring nodes is ensured by observing their contribution to packet forwarding mechanism. To implement the trust derivation mechanism, Trust Update Interval (TUI) of each forwarded packet is buffered in the node as (GPSR Agent::buffer packet). The TUI is a very critical component of such a trust model. It determines the time a node should wait before assigning a trust or distrust level to a node based upon the results of a particular event. After transmission, each node promiscuously listens for the neighboring node to forward the packet.

3.2 Enhanced greedy perimeter stateless routing (EGPSR)

EGPSR selects an adjacent neighbor that has the least distance to a particular destination. In contrast to GPSR, secured greedy perimeter stateless routing (S-GPSR) introduced the concept of trust level which resulted a more secured routing over a geographical area or over a location based routing. But again S-GPSR lacked in terms of efficiency as a common or constant trust update interval for several nodes may be troublesome in case of heavy traffic. Efficient greedy perimeter stateless routing (E-GPSR) introduces the concept of “observation time (ot)” for each node separately in addition to the trust level.

4. RESULTS AND DISCUSSION

Enhanced greedy perimeter stateless routing protocol is implemented for mobile radio network with different coverage area considering 100 and 150 number of nodes for simulation as in Figure 2. The communication and intercommunication between the nodes are explained and projected in Figure 3 and Figure 4. It is compared with secured greedy perimeter stateless routing protocol for different number of malicious nodes. The results show that on the average, the routing overhead achieved using the E-GPSR protocol was 70% less than the standard S-GPSR protocol.

Table 3. Simulation Parameters

Parameter	Value
Simulation tool	NS2
Number of nodes	100-150
Coverage distance	150-200 km
Control packets	<100

An improvement of 25% in the delivery ratio has been achieved in the E-GPSR protocol. The improvement in the above mentioned network performance is mainly due to smaller trust values, shorter routing decisions and less number of control packets taken by the trust based model implemented in GPSR to get rid of the interference as in Figure 5.

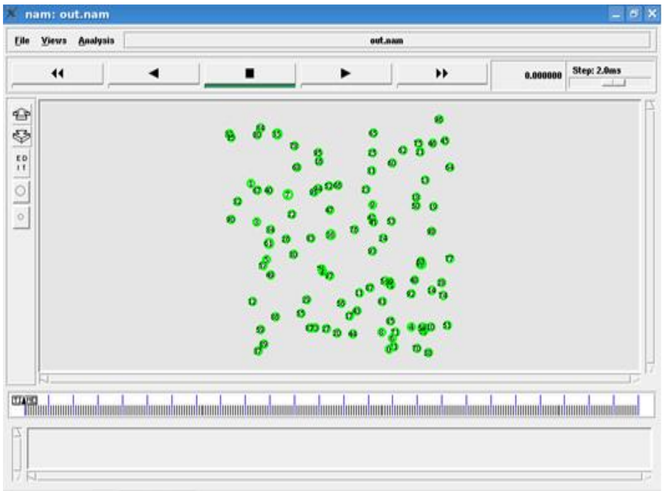

Figure 2. Node initialization

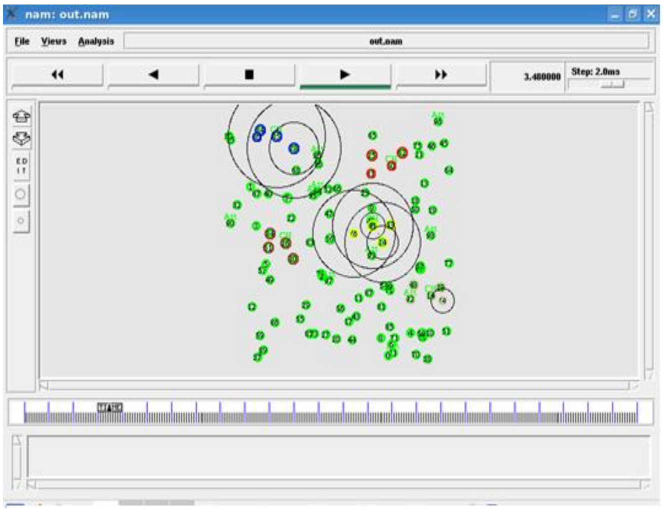

Figure 3. Communication between the nodes

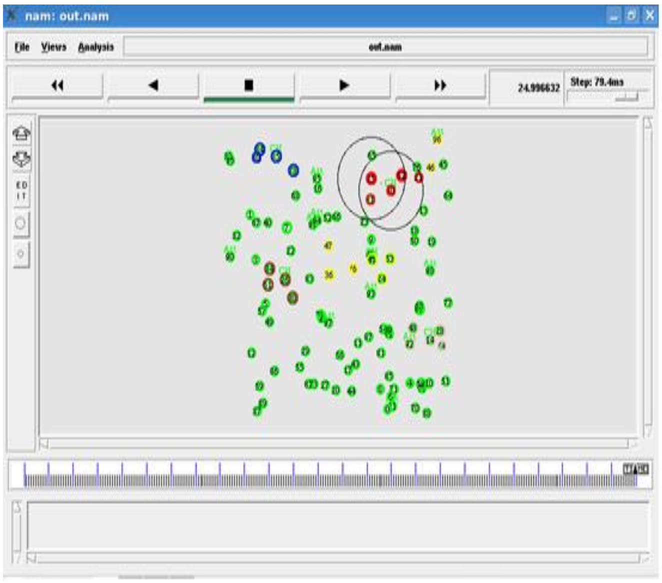

Figure 4. Intercommunication between nodes

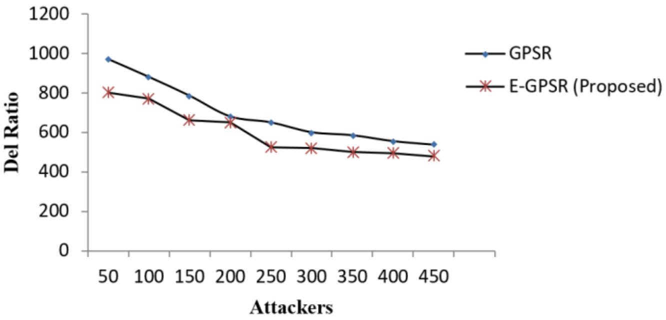

Figure 5. Attackers Vs DelRatio

Attackers try to hack to the network nodes resulting in delay of packets delivery. Figure 5 shows the statistical analysis of attackers and delivery of packets. On comparing the delivery ratio between these two routing algorithms, it is observed that the proposed EGPSR is better for the increased number of attackers.

Attackers try to hack to the network nodes resulting in transmitting energy getting reduced to reach destination nodes. Figure 6 shows the statistical analysis of attackers Vs energy. It is inferred that the proposed scheme provides minimum energy consumption even for the larger number of attackers with the network.

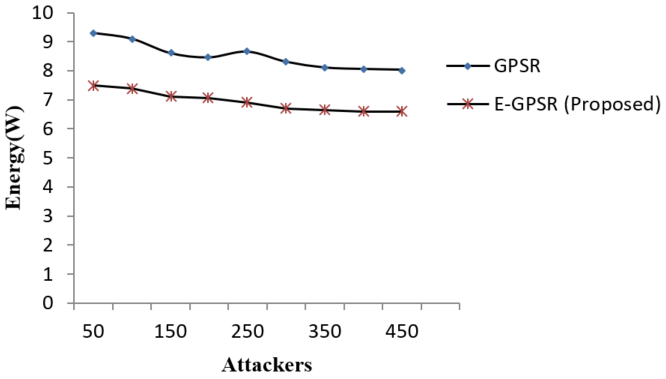

Figure 6. Attackers Vs energy

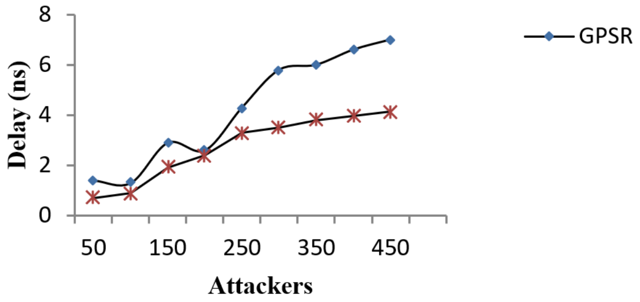

Figure 7. Attackers Vs delay

Attackers track the destination node and try to interfere with the transmitter, which ensures in calculating the delay in the network. Figure 7 depicts the above statement. Minimum delay in the network persists for larger number of networks in EGPSR compared with GPSR.

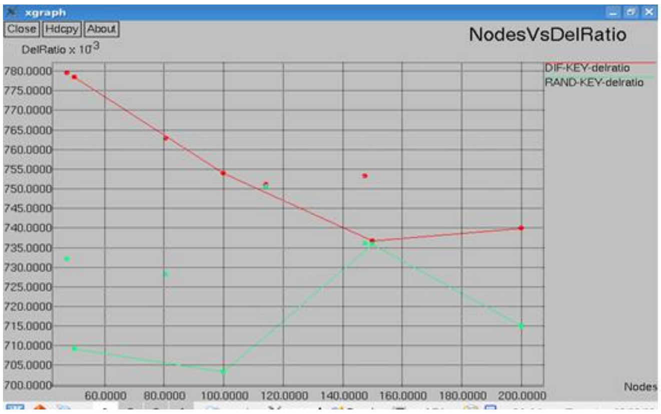

Figure 8. Nodes Vs delay ratio

Considering various node in the network and its delivery ratio. Key management helps in finding the free users in the network. Figure 8 shows that the distributed key produces better than the Random key mechanism.

Figure 9 projects that the energy emitted by distributed is less compared with random, which makes the proposed scheme a better way.

Figure 10 and Figure 11 clearly project the beauty of the proposed scheme. Overhead to the node and delay created at node are compared and proved.

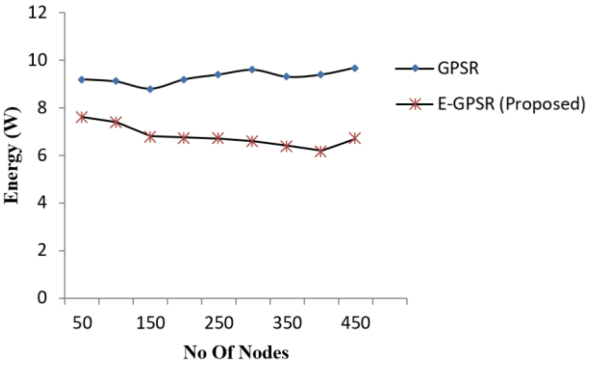

Figure 9. Nodes Vs energy

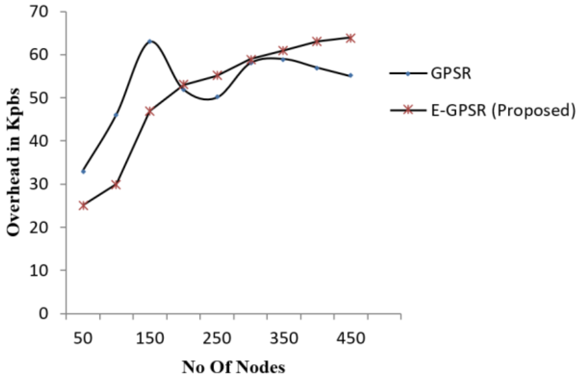

Figure 10. Nodes Vs Overhead

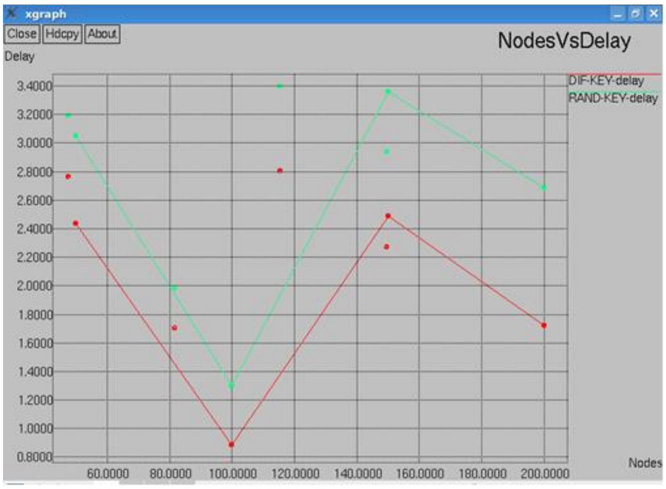

Figure 11. Nodes Vs delay

5. CONCLUSION

In this paper, the issue of providing end to end secured communications in randomly deployed Cognitive Radio Networks, via differentiated key pre distribution, where the idea is to distribute different number of keys to different nodes to enhance the resilience of certain links in the network. This feature is leveraged during routing, where nodes route through links with higher resilience. End to end secure communication protocol based on the above methodology by extending well known location centric (GPSR) and data centric (minimum hop) routing protocols are presented. Detailed theoretical analysis and performance evaluations demonstrate the strengths of the techniques.

REFERENCES

[1] Eschenauer L, Gligor VD. (2002). A key-management scheme for distributed sensor networks. in Proc. of 9th ACM Conf. Comput. Commun. Security, ACM, NewYork, USA: 41-47.

[2] Chan H, Perrig A, Song D. (2003). Random key pre distribution schemes for sensor networks. In Proc. IEEE Symp. Research Security Privacy, MA. Kluwer, Norwell: 197-213.

[3] Du W, Deng J, Han YS, and P. K. Varshney (2005). A pairwise key pre distribution scheme for wireless sensor networks. ACM Trans. Inf. Syst. Security 8(2): 228-258.

[4] Lee J, Stinson DR. (2004). Deterministic key pre distribution schemes for distributed sensor networks. In Proc. 11th Workshop Sel. Areas Cryptography, Waterloo, Canada, 294-307. https://doi.org/10.1007/978-3-540-30564-4_21

[5] Lee J, Stinson DR. (2005). A combinatorial approach to key pre distribution for distributed sensor networks. in Proc. IEEE Wireless Commun. Netw. Conf., Mar., 13-17. https://doi.org/10.1109/WCNC.2005.1424679

[6] Liu DG, Ning P. (2005). Establishing pairwise keys in distributed sensor networks. In ACM Trans. Inf. Syst. Security 8(1): 41-77. https://doi.org/10.1145/948109.948119

[7] Zhu S, Xu S, Setia S, Jajodia S. (2003). Establishing pairwise keys for secure communication in ad hoc networks: a probabilistic approach. In Proc. 11th IEEE International Conf. Netw. Protocols, Atlanta, GA, 326-335. https://doi.org/10.1109/ICNP.2003.1249782

[8] Landstra T, Zawodniok M, Jagannathan S. (2007). Energy-efficient hybrid key management protocol for wireless sensor networks. In IEEE Conf. Local Comput. Netw., Rolla, MO, 559-562. https://doi.org/10.1109/LCN.2007.64

[9] Gaafar M, Khafagy MG, Amin O, Alouini MS. (2016). Improper Gaussian signaling in Full duplex relay channels with residual self-interference. Proc. IEEE Int. Conf. Commun. (ICC), Kuala Lumpure, May. https://doi.org/10.1109/ICC.2016.7511009

[10] Sboui L, Ghazzai H, Rezki Z, Alouini MS. (2015). Achievable rate of a cognitive MIMO multiple access channel with multi-secondary users. IEEE Communications Letters (19): 403-406. https://doi.org/10.1109/LCOMM.2014.2387843

[11] Wang L, Kim KJ, Duong TQ, Elkashlan M, Poor HV. (2015). Security enhancement of cooperative single carrier systems. IEEE Transactions on Wireless Communications 10(1): 90-103. https://doi.org/10.1109/tifs.2014.2360437

[12] Yang WW, Zhao XH. (2017). Robust resource allocation for orthogonal frequency division multiplexing-based cooperative cognitive radio networks with imperfect CSI. IET Communications 11(2): 273-281. https://doi.org/10.1049/iet-com.2016.0742

[13] Kim SJ, Soltani N, Giannakis G. (2013). Resource allocation for OFDMA cognitive radios under channel uncertainty. IEEE Transactions on Wireless Communications 12(7): 3578-3587. https://doi.org/10.1109/TWC.2013.062413.121892

[14] Kailkhura B, Nadendla VSS, Varshney PK. (2015). Distributed inference in the presence of eavesdroppers: A survey. IEEE Communications Magazine 53(6): 40-46. https://doi.org/10.1109/MCOM.2015.7120015

[15] Elkashlan M, Wang L, Duong TQ, Karagiannidis GK, Nallanathan A. (2015). On the security of cognitive radio networks. IEEE Transactions on Vehicular Technology 64(8): 3790-3795. https://doi.org/10.1109/TVT.2014.2358624

[16] Cai Y, Mo Y, Ota K, Luo C, Dong M, Yang LT. (2014). Optimal data fusion of collaborative spectrum sensing under attack in cognitive radio networks. IEEE Network 28(1): 17-23. https://doi.org/10.1109/MNET.2014.6724102

[17] Najimi M, Ebrahimzadeh A, Andargoli S, Fallahi A. (2013). A novel sensing nodes and decision node selection method for energy efficiency of cooperative spectrum sensing in cognitive sensor networks. IEEE Journal on Sensors 13(5): 1610-1621. https://doi.org/10.1109/JSEN.2013.2240900

[18] Zou Y, Champagne B, Zhu WP, Hanzo L. (2015). Relay-selection improves the security reliability trade-off in cognitive radio systems. IEEE Transactions on Communications 63(1): 215-228. https://doi.org/10.1109/tcomm.2014.2377239

[19] Deng X, Haimovich AM. (2005). Power allocation for cooperative relaying in wireless networks. IEEE Communication Letters (9): 994-996. https://doi.org/10.1109/LCOMM.2005.11012

[20] Yang J, Ulukus S. (2012). Optimal packet scheduling in an energy harvesting communication system. IEEE Transactions on Communications 60(1): 220-230. https://doi.org/10.1109/tcomm.2011.112811.100349

[21] Wu YQ, Hu F, Zhu YY, Kumar S. (2017). Optimal Spectrum handoff control for cognitive radio network based on hybrid priority queuing and multi teacher apprentice learning. IEEE Transactions on Vehicular Technology 66(3): 2630-2642.

[22] Xu XM, Yang WW, Cai YM. (2017). Opportunistic relay selection improves reliability-reliability tradeoff and security-reliability tradeoff in random cognitive radio networks. IET Communications 11(3): 335-343. https://doi.org/10.1049/iet-com.2016.0702

[23] Malathi P, Vanathi PT. (2008). OFDM for wireless local area network systems. AMSE Journals, Series Advances B51(1): 1-16, 26.

[24] Perarasi T, Nagarajan G, Abinaya P. (2016). Controlled channel sharing for Cognitive Radio networks. Australian Journal of basic and applied Sciences 10(12): 82-90, 29.