International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume1, Issue 8 (November '2015)

A TRUST BASED CR-MANET ROUTING PROTOCOL

T.Parameswaran,
Teaching Fellow, Department of CSE,
Anna University Regional Centre,
Coimbatore, India.

Dr.C.PalaniSamy,
Professor and Head,
Department of Information Technology,
Bannari Amman Institute of Technology,Erode,India.

G.Shenbagavalli,
PG Scholar,
Department of Computer Science and Engineering,
Anna University Regional Centre,
Coimbatore, India.

Abstract: Cognitive radio is a emerging technology to solve the problems of spectrum inefficiency, and scarcity by providing the vacant channel to the secondary users without disturbing the primary users. This paper presents Gymkhana, multi path route discovery algorithm for cognitive radio mobile ad hoc networks. Data traffic congestion in the network can be avoided by reducing the number of paths from source to destination. From the result of the routing algorithm trust value can be calculated. In the proposed trust based CR-MANET routing protocol, the trust model involves two components: trust value from direct observation and trust value from indirect observation. With direct observation from an observer node, the trust value calculated using Bayesian inference, which is a type of uncertain reasoning when the full probability model can be defined. On the other hand, with indirect observation, the trust value is obtained from neighbor nodes of the source of Secondary user, the trust value is derived using the Dumpster-Shafer theory, which is another type of uncertain reasoning Combining these two trust values, obtain more accurate trust values of the observed nodes in CR-MANETs.

Key words: Cognitive radio Mobile ad hoc Networks, Channels, Trust Model, Packets.

I. INTRODUCTION

Cognitive radio provides intelligent radios that can adapt to their environment. Many research is currently underway on developing many reasoning and learning algorithms that allow cognitive radios to operate in a variety of different situations. Many new technologies initially does not focused on security aspects of cognitive radio. Typically security is always "attached on" after the fact by addin some sort of link authentication and encryption. This works well under data traversing for a wireless network. Since cognitive radios can adapt with the environment and change how they commugnicate, it's very effective that they select optimal, secure communications. Data integrity and confidentiality can be handled in the higher-layer cryptographic security, so here to focus on attacks fundamental to the cognitive radio wireless nodes itself, and independent of its higher-layer communications techniques. By putting artificial intelligence (AI) engines in charge of our wireless devices, need to be aware that these engines can be provided false sensory input by adversaries, and this false input affects its beliefs and behavior. challenging research topic. There are two approaches provide security in CR-MANET. Prevention based approach and detection based approach. In this detection based approach is a on demand routing protocol approach to provide security dynamically during the packet delivery.

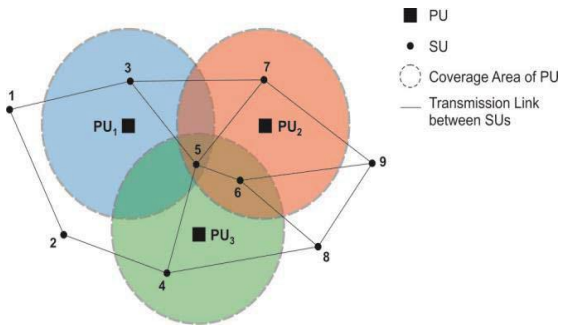

Figure 1: System model

CR-MANET has a popular communication technology in military tactical environments such as establishment of communication networks used to coordinate military network,emergency network,cellular network, vehicles, and operational command centers. Security in CR-MANET is a

II. RELATED WORK

a) Reputation-Based Schemes

Reputation-based schemes attempt to identify the malicious nodes that drop packets with a rate more than a predefined threshold in order to avoid them in routing. This system adopts the local reputation value. Each node keeps the reputation value of its k-hop neighborhood and the value is exchanged in k-hop neighborhood. This method helps to fully learn the experiences from its neighbor which helps to improve the ability to judge and improve itself.

Neighborhood cooperation plays major role than the remote node, hence the node need not record the reputation of the remote node. If the node record reputation of 1-neighborhood, when the node moves from the area, the reputation will be lost. If a node record has its k-neighborhood reputation, the node can learn the experiences from local areas .Reputation-based schemes suffer from false accusations where some honest nodes are falsely identified as malicious. This is because the nodes that drop packets temporarily, e. g., due to congestion, may be falsely identified as malicious by its neighbors. In order to reduce the false accusations, the schemes should use tolerant thresholds to guarantee that a node's packet dropping rate can only reach the threshold if the node is malicious. However, this increases the missed detections where some malicious nodes are not identified. Moreover, tolerant threshold enables the nodes with high packet dropping rate to participate in routes, and enables the malicious nodes to circumvent the scheme by dropping packets at a rate lower than the scheme's threshold. When a node's reputation value is above the threshold, it does not have incentive to relay packets because it does not bring more utility.

b) Payment Schemes

Payment (or incentive) schemes use credits (or micropayment) to encourage the nodes to relay others' packets. Since relaying packets consumes energy and other resources, packet relaying is treated as a service which can be charged. The nodes earn credits for relaying others' packets and spend them to get their packets delivered. In Sprite, for each message, the source node signs the identities of the nodes in the route and the message. Each intermediate node verifies the signature and submits a signed receipt to Trusted parties to claim the payment. However, the receipts overwhelm the network because one receipt is composed for each message. To reduce the receipts' number, PIS generates a fixed size receipt per route regardless of the number of messages. In ESIP, the payment scheme uses a communication protocol that can transfer messages from the source node to the destination with limited use of the public key cryptography operations. Public key cryptography is used for only one packet and the efficient hashing operations are used in next packets. Unlike ESIP that aims to transfer messages efficiently, E-STAR aims to establish stable and reliable routes.

c) Trust systems

The issue of evaluating the trust level as a generalization of the shortest path problem in an oriented graph, where the edges correspond to the opinion that a node has about other node. The main goal is to enable the nodes to indirectly build trust relationships using exclusively monitored information. In, Velloso et al. have proposed a human-based model which builds a trust relationship between nodes in ad hoc network. Without the need for global trust knowledge, they have presented a protocol that scales efficiently for large networks. In, Lindsay et al. have developed an information theoretic framework to quantitatively measure trust and model trust propagation in ad hoc networks.

III. ROUTING PROTOCOLS FOR CR-MANET

In this section, survey of state – of – the – art routing protocols for Mobile Cognitive Radio Ad Hoc Networks are presented. The authors consider the routing protocol for the last three years. The Classification is based on: Multi – channel usage, Link Modeling, Geographic routing, Spectrum awareness, Connectivity and Clustering. The Classification of the routing protocols is presented in the Figure 2.

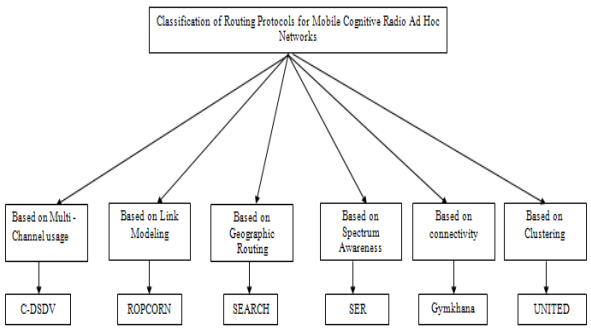

Figure 2: Classification of Routing Protocols for Cognitive Radio Mobile Ad Hoc Networks.

a) **Based on Channel Switching**

Switching of channel frequently occurs when a node wants to change its channel as it has more than two routes to the destination in different channels. It is based on **C-DSDV Protocol** The protocol is a pre - active cognitive multi – channel routing protocol which utilizes multiple channels in the CR ad hoc networks [8]. The routing and the channel allocation are the two main challenges in CR ad hoc networks, which are considered here in this paper. It aims at optimizing the system performance of multi-hop CR ad hoc networks, by using a cross – layer design approach. The protocol is the enhanced version of the already existing DSDV (Destination Sequenced Distance Vector) protocol, for cognitive routing scheme. Function of the C-DSDV protocol: Each node in the CR ad hoc network maintains a routing table with all possible destinations, and the number of routing hops to each destination is recorded. Therefore the routing information is present every time, even if the source node requires a route or not. Routing table updates are sent periodically throughout the network to maintain the table consistency. New route broadcasts will contain the address of the destination node, the number of hops to reach

the destination, the sequence number of the information received about the destination. The sequence number will unique for each broadcast and the route with the updated sequence number is always used for broadcasting. The nodes will transmit the updates immediately if new information arrives or a change in the topology or a switch in the channel. There is a possible of delaying the route advertisement but the channel change is advertised immediately to all other nodes in the network.

b) **Based in Link Modeling**

Links are formed during the communication among the two nodes in a network. The link connectivity and disconnectivity plays an important role in the cost metric.The scheme based on **ROPCORN Protocol**. The protocol was designed for data transportation by making use of link modeling. Two routing metrics are considered for this purpose. They are spectrum availability cost and load estimation. Aim is to maximize the data rates and minimize delay and the total resources consumed, for a set of communication sessions. The following example reveals the protocol approach.

c) **Geographic forwarding**

The idea is to discover several paths, which are combined at the destination to form the path with the minimum hop count. The nodes used in this approach will be equipped with GPS devices. It is based on **SEARCH Protocol - Spectrum Aware Routing protocol** The SEARCH protocol uses the geographic forwarding. This protocol jointly considers the path and the channel selection to avoid the regions of the Primary User activity during the route formation. Minimization of hop count to reach the destination is done by using the optimal path found by geographic forwarding . The idea of the geographic forwarding is used in this protocol. It is able to deal with reasonable levels of PU activity changing rate. Also, a mechanism for disseminating the destination location both at the source and at each intermediate node is required.

The protocol assumes the primary users activities in an ON/OFF process. The functions followed by the protocol are (1) Route setup phase (2) Joint Channel – Path optimization phase and (3) Route Enhancement, in order to improve the route during its operation.

a) **Based on Spectrum Awareness**

The key factor of spectrum aware routing is the combination of spectrum discovery and the route discovery in MCRAHNs. Based on **SER - Spectrum and Energy Aware Routing Protocol**

The main aim of this protocol to establish a bandwidth guaranteed QoS routes in small CR networks where the topological changes are low. The protocol uses Time Division Multiple access The QoS requirement considered here is the number of transmission timeslots for a packet on its route from source to reach the destination. Working of SER protocol**:** The SER is an on demand routing protocol proposed for multihop CR networks. The basic operation of SER includes route discovery, data transmission and route maintenance.

b) **Based on Connectivity**

Connectivity in CR-MANET based on **GYMKHANA Protocol**. The protocol that is capable of identifying the network connectivity towards the destination is the Gymkhana protocol. It is a routing protocol that identifies all possible paths of connectivity towards the destination. The protocol forwards the information in the path which is not affected by the network zone, as it does not support the network stability and connectivity. For this purpose, a mathematical framework based on Laplacian spectrum graphs, is used for the evaluation of the different routes of the CR network. It is a distributed protocol and it is able to measure the connectivity of different network paths and to forward the data packets among the different paths which avoid the network zones. Therefore, by evaluating the activity of the PUs, a path is determined with the highest connectivity.

a) **Based on Clustering**

Here, a distributed and efficient cluster-based spectrum and interference aware routing protocol is proposed, which incorporates the spectrum availability cost and interference metrics into the routing algorithm to find better routes. The mechanism based on **UNITED NODE Protocol** For this protocol, a mobile CR ad hoc network environment with a number of primary and secondary nodes, where all nodes communicate with each other in their own networks, is considered. There is no communication (i.e. no cooperation) between primary and secondary networks. A novel algorithm, united nodes (UNITED), is proposed for maximizing the network throughput and minimizing the end-to-end delay. The UNITED operates autonomously in a distributed manner at every node. Initially, the nodes organize themselves into several clusters by the clustering algorithm that is based on location, communication efficiency, network connectivity and spectrum availability. After the completion of cluster formation, routing is done according to the spectrum usage and interference metrics. Clusters adapt themselves dynamically with respect to spectrum availability, and the high mobility of the nodes. The proposed clustering algorithm for mobile CR ad hoc networks makes autonomous decisions in a distributed manner. It is based on a combined weight metric that takes

into account several system parameters such as distance, transmission power, mobility, remaining power of nodes and sensed information about available spectrum.

IV. OVERVIEW OF THE SYSTEM

The network consists of Primary users and secondary users; there are exactly P channels each of which is assigned to a Primary Users. A PU is located in the center of its coverage area and it is assumed that all PUs and SUs are stationary. In the network under consideration, some of the SUs can be in the coverage areas of one or more PUs, while the others are not affected by any PU activity. The SUs out of the influence region of a PU can use the channel associated to that PU at any time without any further limitation. On the other hand, the SUs in an area fully covered by all other PUs' coverage areas have to wait until a channel is vacated by its licensee. The communication between two SUs is possible when the transmission ranges of those SUs intersect. If it is the case, then a transmission link between them is established. For the sake of simplicity, we assume a single data flow in the topology. In other words, there are only one source and one destination in the secondary network. We adopt the Ad hoc On-Demand Distance Vector (AODV) style routing mechanism, namely Gymkhana Routing Algorithm. The main difference between AODV and Gymkhana lies on the fact that Gymkhana permits multiple paths in the route discovery phase.

IV. DESIGN

The proposed system is to develop the secure CR-MANET using the extended Gymkhana operations and Artificial intelligence concept for finding the trust values.

GYMKHANA AND THE PROPOSED MODIFICATION

In spectral graph theory, robustness and stability of a network can be measured through algebraic connectivity, which makes use of adjacency and degree matrices. An adjacency matrix of a graph describes which vertices of this graph are connected to which vertices, whereas the number of vertices a vertex is connected to is represented by a degree matrix.

Gymkhana Routing Algorithm is based on the algebraic connectivity of a graph G, in which the eigenvalues of laplacian matrix L of G are found through the roots of the polynomial $p(\lambda) = \det(L - I \cdot \lambda)$, where I is the identity matrix. The calculated roots $\{\lambda 1, \ldots, \lambda i, \lambda i+1, \ldots\}$ are ordered in increasing order such that λi is smaller than $\lambda i+1$. Second smallest-eigenvalue $\lambda 2$ of L gives information about how well connected the overall graph G is. In case of Gymkhana, an average laplacian matrix E[ILc] is defined, of which generic element is the function of the probability that at least one PU is active.

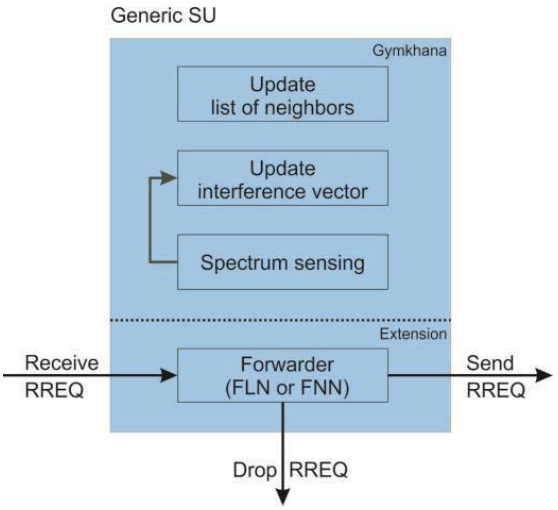

Figure 3: Extension of Gymkhana routing algorithm

we extended the Gymkhana operations performed at a generic SU in order to minimize the number of forwarded RREQs (Fig. 3). The operations carried out at destination remains as it is in. A generic SU periodically updates the list of neighbors and the interference vector in order the capture any changes in the topology. The list of neighbors consists of the nodes, which reside inside the vicinity of that generic SU, whereas the interference vector contains the information of activity factors of PUs which could affect the mentioned SU.

a) Forwarding based on Local Node (FLN)

RREQ message contains the identities (ID) and the list of interference vectors of Secondary Users encountered in any path. In the extended version of Gymkhana, a generic SU can process this RREQ and form a virtual graph VG, consisting of the nodes from source to the generic SU itself. Then, the second-smallest Eigen value of the formed cognitive Laplacian matrix is computed, which is further used in a cognitive utility function with respect to path. The temporal cognitive value function is compared with the best old cognitive utility function value and a decision is taken whether to forward the proceed RREQ or not. Forwarding operation based on local node is summarized in the Algorithm.

Algorithm 1.Forwarding based on Local Node (FLN)

1: Form VG with respect to Request $RREQ_{SUk}$
2: Compute second smallest Eigen value λ_2
3: Calculate temporary UFV value
4: if the temporary UFV is greater than best UFV begin

5: forward $RREQ_{SUk}$
6: Update the best UFV value with temporary UFV value
7: else
8: Drop $RREQ_{Sui}$
9: end

b) Forwarding based on neighbor node (FNN)

Depending on the control messaging mechanism between neighbor SUs, a generic SU can get the information of IntVecs owned by its neighbors. This information which actually contains the PU activities on neighbor nodes is beneficiary, since some of the RREQs can be dropped in earlier stages of the route discovery phase. We assume that this kind of message passing is being used in order to forward RREQs based on neighbor nodes. As it is implied, receiver SU decides to which of its neighbors it should forward the received RREQ.

Algorithm 2. Forwarding based on Neighbor Nodes (FNN)

1: UFV = 0
2: for(j=0; j<=n; j++) begin
3: form VG_j with respect to $RREQ_{Sui}$ and j^{th} neighbore of SU_i
4: compute λ_2 { $E[IL^c]_j$}
5: Calculate $U_j^{c\_Temp}$
6 :if $U_j^{c\_Temp} > \exists\ U_m(1), U_m \in U_j^{c\_Best}$ begin
7: $U_j^{c\_Best} = U_j^{c\_Best} \setminus U_m \cup (U_j^{c\_Temp}, ID_j)$
8: UFV=UFV + 1
9: end
10: for(m=1;m≤LTO; j++) begin
11: forward $RREQ_{Sui}$ to $U_m(2)$,
where $U_m \in U_j^{c\_Best}$
12: end
13: if UFV=0 begin
14: Drop $RREQ_{Sui}$
15: end
16:end

VI.TRUST MODEL IN CR-MANET

Based on the information gained from the routing algorithm trust value can be calculated

Framework of the proposed scheme

Based on the trust model , the frame work of the proposed scheme is shown in Fig. 4. In the trust scheme component, the module of trust evaluation and update can obtain evidence from direct and indirect observation modules and then utilize two approaches, Bayesian inference and DST, to calculate and update the trust values. Next, the trust values are stored in the module of trust repository. Routing schemes in the networking component can establish secure routing paths between sources and destinations based on the trust repository module. The application component can send data through secure routing
paths. The trust from direct observation between an observer node A and an observed node B in this trust scheme can be defined further as

$$T^S AB = \rho T^D AB + (1 - \rho) T^C AB,$$

where ρ $(0 \le \rho \le 1)$ is the weight for data packets;
$T^D AB$ is the trust value based on data packets;
$T^C AB$ is the trust value based on control packets. Trust from indirect observation between an observer node A and an observed node B, denoted as $T^N AB$, can be obtained by DST.

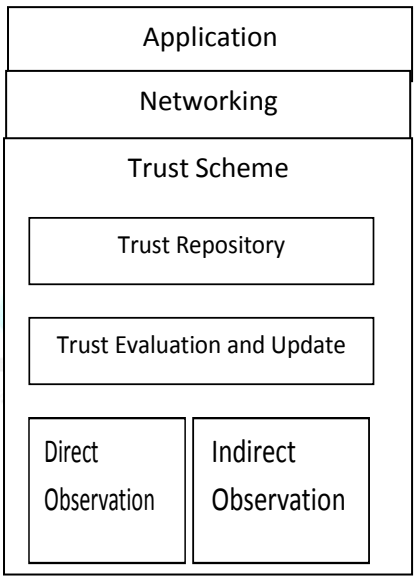

Figure 4: Framework of Trust model

Algorithm 3 Trust Calculation with Direct Observation

1: **if** node A, which is an observer, finds that its one-hop neighbor, Node B that is a trustee, receives a packet **then**
2: the number of packets received increases one
3: **if** node A finds that node B forwards the packet successfully **then**
4: the number of packets forwarded increases one
5: **else**
6: **if** TTL of the packet becomes zero **or** overflow of buffers in node B **or** the state of wireless connection
of node B is bad **then**
7: the number of packets received decreases one
8: **end if**
9: **end if**

10: **end if**
11: calculate the trust value, T_S, and update the old one.

The above algorithm 3 explains the trust value of neighbor nodes. Using the value malicious nodes can be detected.

Algorithm : Trust Calculation with Indirect Observation
if node A, which is an observer, has more than one hop neighbors between it and the trustee, node B **then**
2: calculates the trust value, T_N,
else
4: set TN to 0
set λ to 1
6: **end if**

VII.SECURE ROUTING BASED ON TRUST

The Gymkhana routing information is used to find the trust values of the nodes in the network based on the uncertain reasoning concept. In the routing algorithm the source node send the RREQ and ID of the node to neighbored nodes. The neighbored nodes reply to the source node with RREP message. Using that information trust value can be calculated. The source node send the packets using multi hop neighbors. The trust from multi hop neighbors are calculated. Detect the malicious node and isolate the nodes from the network. Secure routing can be established.

FLOW DIAGRAM

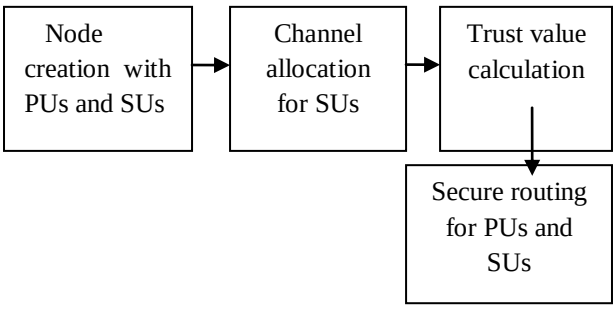

Fig.5: Data flow diagram for CR-MANET with secure routing

VIII. IMPLEMENTATION

The proposed scheme can be simulated in ns-2 simulator with the Gymkhana routing protocol and trust calculation using the artificial intelligence concept. Performance analysis of the proposed extension of Gymkhana routing protocol in terms of multiple paths between any source to destination pair during route discovery. The trust value calculated using the direct observation and indirect observation from observed node. Combination of the trust values more accurate secure route can be established and isolate the malicious from the network.

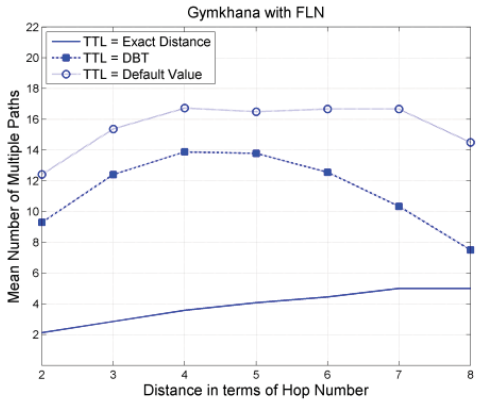

Figure 6: Gymkhana with Forwarding based on Local node.

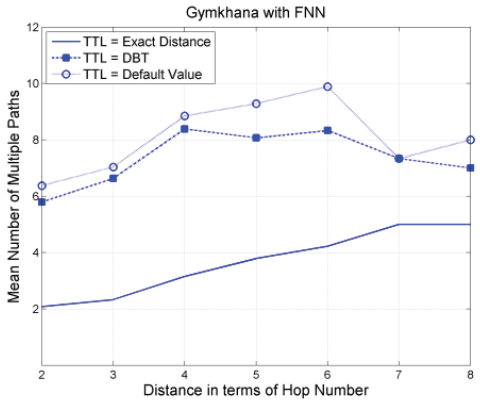

Figure 7: Gymkhana with forwarding based on Neighbor nodes

Using gymkhana routing algorithm with trust calculation is a efficient way of finding the malicious nodes in the network. After finding the malicious nodes in the network isolate the malicious nodes and secure routing can be established.

IX. CONCLUSIONS

In this paper, propose a unified trust management scheme that enhances the security of CR-MANETs. Using the mechanism Dempster-Shafer theory, Bayesian inference, calculate the trust values of observed nodes in CR-MANETs. Misbehavour of nodes can be identified using the trust mechanism. Nodes with lowest trust values can be

identified and isolated. The results of CR-MANET routing scenario positively support the throughput, packet delivery ratio considerably. The future work can be established using various protocols of CR-MANET.

X. REFERENCES

[1] S. Corson and J. Macker, "Mobile ad hoc networking (MANET): routing protocol performance issues and evaluation considerations," IETF RFC 2501, Jan. 1999.

[2] F. R. Yu, Cognitive Radio Mobile Ad Hoc Networks. New York: Springer, 2011.

[3] J. Loo, J. Lloret, and J. H. Ortiz, Mobile Ad Hoc Networks: Curren Status and Future Trends. CRC Press, 2011.

[4] Q. Guan, F. R. Yu, S. Jiang, and V. Leung, "Joint topology control and authentication design in mobile ad hoc networks with cooperative communications," IEEE Trans. Veh. Tech., vol. 61, pp. 2674 –2685, July 2012.

[5] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service (QoS) co-design in cooperative mobile ad hoc networks," EURASIP J. Wireless Commun. Networking, vol. 2013, pp. 188–190, July 2013.

[6] Y. Wang, F. R. Yu, H. Tang, and M. Huang, "A mean field game theoretic approach for security enhancements in mobile ad hoc networks," IEEE Trans. Wireless Commun., vol. 13, pp. 1616–1627, March 2014.

[7] J. Chapin and V. W. Chan, "The next 10 years of DoD wireless networking research," in Proc. IEEE Milcom'11, (Baltimore, MD, USA), Nov. 2011.

[8] S. Bu, F. R. Yu, P. Liu, P. Manson, and H. Tang, "Distributed combined authentication and intrusion detection with data fusion in high-security mobile ad hoc networks," IEEE Trans. Veh. Tech., vol. 60, pp. 1025–1036, Mar. 2011.

[9] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: distributed key management for security," in Proc. 2nd OLSR Workshop, (Domaine de Voluceau, France), Dec. 2005.

[10] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing mobile ad hoc networks with certificateless public keys," IEEE Trans. Dependable and Secure Computing, vol. 3, pp. 386–399, Oct.–Dec. 2006.

[11] Y. Fang, X. Zhu, and Y. Zhang, "Securing resource-constrained wireless ad hoc networks," IEEE Wireless Comm., vol. 16, no. 2, pp. 24–30, 2009.

[12] F. R. Yu, H. Tang, P. Mason, and F. Wang, "A hierarchical identity based key management scheme in tactical mobile ad hoc networks," IEEE Trans. on Network and Service Management, vol. 7, pp. 258 – 267, Dec. 2010.

[13] FCC, "Spectrum policy task force report," in Federal Communications Commission (FCC 02), Washington, DC, USA, pp. 745–747, Nov. 2002.

[14] J. Mitola III, "Cognitive radio for flexible mobile multimedia communication," in Proc. the IEEE International Workshop on Mobile Multimedia Communications, pp. 3–10, November 1999.

[14] I. F. Akyildiz, W. Lee, M. C. Vuran, S. Mohanty, "Next generation/dynamic spectrum access/cognitive," Computer Networks J., vol. 50, pp. 2127–2159, 2006.

[15] K. R. Chowdhury, I. F. Akyildiz, "CRP: A Routing Protocol for Cognitive Radio Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 29, no. 4, April 2011.

[16] A. S. Cacciapuoti, C. Calcagno, M. Caleffi, L. Caleffi, "CAODV: Routing in mobile ad-hoc cognitive radio networks," Wireless Days, 2010 IFIP , pp.1-5, 20-22 Oct. 2010.

[17] S. M. Kamruzzaman, Eunhee Kim, Dong Geun Jeong , "An energy efficient QoS routing protocol for cognitive radio ad hoc networks," 13th International Conference Advanced Communication Technology,pp.344-349, 13-16 Feb. 2011.

[18] P.Paweczak, "Protocol Requirements for Cognitive Radio Networks," TU Delft, AAF Deliverable, 2005.

[19] S. Abdelaziz, M. ElNainay, "Metric-based taxonomy of routing protocols for cognitive radio ad hoc networks," Journal of Network and Computer Applications, vol. 40, pp. 151-163, April 2014

BIOGRAPHY

Parameswaran.T has received his B.E degree in Electronics and Communication Engineering from Velalar College of Engineering and Technology, Erode, and M.E degree in Software Engineering from College of Engineering Guindy, Anna

University Chennai in 2005 and 2008 respectively. He is currently pursuing his Ph.D Anna University Chennai. He is currently working as Teaching Fellow in the Department of Computer Science and Engineering, Anna University Regional Campus, Coimbatore, Tamilnadu, India.

Palanisamy.C has received his B.E degree in Electronics and Communication Engineering from University of Madras, Chennai and M.E degree (Gold Medalist) in Communication Systems from Thiagarajar College of Engineering, Madurai, Madurai Kamaraj University in 1998 and 2000 respectively. He has received his Ph.D from the faculty of Information and Communication Engineering, Anna University, Chennai in 2009. He has more than 15 years of academic and research experience and currently he holds the post of Professor and Head of the Department of Information Technology, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India. He has published more than 40 research papers in various journals and conferences. He has organized more than 15 workshops and holds 2 funded projects. He is a lifetime member of ISTE. He Won Best M.E Thesis Award at Thiagarajar College of Engineering, Madurai and best paper award titled, "A Neural Network Based Classification Model Using Fourier and Wavelet Features," Proceedings of the 2nd Int. Conf. on Cognition and Recognition 2008, (ICCR 2008), Organised by P. E. S. College of Engineering, Mandaya, Karnataka, India, pp. 664-670, 2008. His research interests include Data mining, image processing, and mobile networks.

Shenbagavalli.G has received his B.E degree in Computer Science and Engineering from University College of Engineering,Arni. She is currently pursuing her M.E degree in Software Engineering from Anna University Regional Campus, Coimbatore. Tamilnadu, India.