International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 8 (2015) pp. 19367-19387

http://www.ripublication.com

Towards Security In Cognitive Radio Networks

Suhasini Sodagudi and Prof. Rajasekhara Rao Kurra

Associate Professor, Department of Information Technology
VR Siddhartha Engineering College, Vijayawada, A.P, India
Ssuhasini09@gmail.com
Director, Sri Prakash College of Engineering, Tuni
Sri Prakash College of Engineering, Rajahmundry, A.P. India
krr@sriprakash.org

ABSTRACT

Information inside a MANET moves around a communication devices and mobile nodes through an intermediary join wireless, without any pre-defined infrastructure or central authority control. This unavailability of central administration is one of the major key features of the network from intruders. Therefore, at all times, security issues in MANET are being a difficult task thus binding itself more vulnerable to attacks. Among these vulnerabilities, behavior attacks are more dangerous since they affect and reduce network performance. Cognitive network can offer chances to the new users called secondary users. This technology created mainly as a remedy for which are not licensed users to uses the available licensed transmission. Little research regarding security has been done in such technology. However, a selfish node can take control of all or some part of the resources of different channels, forbidding other nodes from accessing these resources. Selfish attacks are dangerous security problem because they gradually decrease the performance of a cognitive network. Hence there is a need for a proposed system to identify new selfish attacks in cognitive radio ad-hoc networks and packet drop attacks, one of the DOS attack in which a router that is supposed to relay packets instead discards them. This work emphasizes in detection of these attacks using the routing protocols. A detailed analysis of the impact of such attacks will be considered to show the necessary preventive measures.

General Terms Ad hoc, vulnerabilities, behavior

Keywords Lightweight Cryptography, MANET, Cognitive Radio Network.

1. INTRODUCTION

A mobile ad hoc network is a type of network without central authority control, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move without depend in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use. Cognitive network is a type of ad hoc network technology which offers communication facilities to new users known as secondary users. Earlier, this communication technology was introduced as a remedy for unlicensed users to use the available resources like bandwidth and radio frequency. These resources serve for fast development and deployment of mobile devices, where MANET becomes an important component of modern distributed system.

CR (Cognitive radio) technology is contemplated to solve the problem in wireless networks resulting from the limited available spectrum and inefficiency in the spectrum usage by exploiting the existing wireless spectrum opportunistically. CR ad hoc network has been recently attracted many researchers based upon their interest. In this network, security has been given much importance. Based upon the security level in the network, still several problems are raising due to threats and vulnerabilities. Figure 1 shows the difference between the normal mobile frequencies and the Cognitive Radio network frequencies. The main goal in Cognitive Radio network is that a user has a provision to use any channel to carry their data. That's why the traffic is not crowded in this network when compared to the normal scenario. It is observed in figure 1 that the channels are nothing but the mobile, wireless and the sensors. So the Cognitive network can perform the communication between any networks.

2. COGNITIVE RADIO SCENARIO

The concept of cognitive radio was first proposed by Joseph Mitola III in a seminar at KTH(the Royal Institute of Technology) in 1998. Depending on transmission and reception parameters, there are mainly two types of cognitive radio's:

- Full (Mitola Radio) : This cognitive can be any wireless device
- Spectrum Sensing Cognitive Radio : This cognitive can use the frequencies of the radio instead of the wireless that can be called as a sensing devices.

[15]Cognitive-radio networks aim to use the spectrum in a dynamic manner by allowing radio terminals to operate in the best available frequency band, maintaining seamless communication requirements during transitions to better spectrum. Figure 2 describes the cognitive radio concept and it is seen that information can be sent both through base station and without base station also. If without base station is considered then, a newpath, called as the cognitive radio is used. Now the users are called as secondary users. Thus the technology serves as a remedial approach for unlicensed users to use available resources for fast development and deployment of mobile devices to form an ad hoc network. In mobile ad hoc networks when used in network-centric operations, there is a growing need for a systematic methodology for analyzing/predicting the performance of the network over the mission duration. With

the advance in cognitive networking as a possible means of exploiting unused spectrum, there is now a growing need to study how to design a cognitive network using an automated methodology. A cognitive radio is an intelligent radio that can be programmed and configured dynamically.[14]

Its transceiver is designed in such a way that it can use the best wireless channels in its vicinity. Such a radio automatically detects available channels in wireless spectrum, then accordingly changes its transmission or reception parameters to allow more concurrent wireless communications in a given spectrum band at one location. This process is a form of dynamic spectrum management.[11] CR technology is generally used for dynamic spectrum sharing (DSS) and addresses the problem of spectrum scarcity. The spectrum in CR is applicable to the following contexts:

- Spectrum sharing - allow cognitive radio users to share the spectrum bands of the licensed-band users. However, the cognitive radio users have to restrict their transmit power so that the interference caused to the licensed-band users is kept below a certain threshold. Thus, capable of using bands assigned to licensed users and unlicensed parts of the radio frequency (RF) spectrum
- Spectrum mobility - Process by which a cognitive-radio user changes its frequency of operation.
- Radio environment – which provides all capabilities for a wireless node with RF spectrum
- Spectrum decision - Based on the spectrum sensing, cognitive radio users decide their transmission strategies. If the licensed users are not using the bands, cognitive radio users will transmit over those bands. If the licensed users are using the bands, cognitive radio users share the spectrum bands with the licensed users by restricting their transmit power.
- Spectrum sensing - cognitive radio users first listen to the spectrumallocated to the licensed users to detect the state of the licensed users.

As shown in the architecture of the cognitive radio network, there exist two classes of networks namely CR with infrastructure and CR without infrastructure. In CR with infrastructure, information exchange takes place through basestation and in without infrastructure case, communication exists through a new path which is cognitive radio setup using an automated methodology.In the above, figure 1 reveals that the spectrum is available to primary users and the CR (Cognitive Radio) users. [12]The users may occupy the spectrum on some portions within the spectrum. In this diagram, dark greenish-blue color shows the occupied area of the primary users and the empty lines shows the idle spectrum band, which is unused. Also, two types of CR users A and B are shown.The sub channels are allocated to the both the users in this manner.

- Spectrum Sensing - Initially trace which parts of the spectrum are available
- Spectrum Decision - Pick up the efficient presented channel
- Spectrum Sharing - Cooperate access to this type channel with the other users
- Spectrum Mobility – Leave the channel when a premium user is presented

As shown in figure 2, the Cognitive network communicate with in the different types of

networks, those are the Sensor network, [7][3]Mesh network and Mobile ad hoc network the characteristics of Cognitive Radio includes

- Cognitive Capability - Identify the unused spectrum at a specific time or location (Spectrum Holes/ White Spaces)
- Re-configurability - Sending and Receiving different types of frequencies. Use various access technologies.

3. SECURITY CHALLENGES IN COGNITIVE RADIO

Security is very essential component to be included in every communication networks. To possess it, one needs to assess the pros and cons existing in the system or any model. Elaborately speaking security threats need to be identified. [8]These are the areas of attacks that can take place. In this context, following are the various types of attacks against CRs and CRNs

- Incumbent Emulation (IE) attacks – these attacks exist in 2 cases :
- Selfish IE attack - secondary's can avoid accessing a band if an incumbent signal is detected in the band, an attacker can preempt and monopolize a fellow band if it manages to fool others into believing that it is an incumbent.[18][6]
- Malicious IE attack - suppress legitimate secondary's from accessing spectrum, thereby causing denial of service.[1][6]
- Spectrum Sensing Data malicious attacks - a portion of the spectrum band may be used both by primary and secondary users and occupy the licensed bandwidth. Hence selfish behavior is revealed from such attacks.
- Cross layer type attacks – attacks are initiated at MAC layer and are aimed at routing due to lack of interaction between the MAC and network layer.[]
- Spectrum Sensing Data Falsification attack (SSDF)- Falsie secondary users can take chance of the cooperative sensing spectrum and introduce SSDF attacks to send false local spectrum sensing results to others, resulting in a wrong spectrum sensing decision.

Mainly there are three types of attack models reflecting selfish behavior aspect as Selfish SSDF, Interference SSDF and Confusing SSDF. From these attacks, it is emphasized to work towards selfish attack detection technique in cognitive radio networks for which selfish behavior is the main argument.

A. SELFISH – ATTACKS

Selfish attack is the one of the attack in the MANET, and it is DoS type of attack and Man – in –the - middle attack. [18]Selfish attacks are the attacks launched by the nodes that possess selfish behavior. A node is said to act "selfish" if any of the given conditions hold :

- Held up the resources for longer duration.
- Providing wrong channel and fake information to other nodes
- Does not cooperate in the network

In Cognitive radio ad hoc networks, selfish node attacks are dangerous, as it can be caused because of the abnormal behavior of the node[3]. In this work, it is proposed with a new mechanism for misbehavior detection to identify selfish nodes in CR network. These attacks can take place in real time environment in the following applications:

Application 1:
Online streaming video like "YouTube" access to users

In this application, the attack may occur due to the licensed and unlicensed users. For instance the YouTube videos are available for access with some conditions. So if any violence issue had happened, it must be restricted. Similarly, the unsociable contents must also possess such restrictions based upon age and mail-id.

Application 2:
IEEE papers restricting to users based on their account types.

In this application, in order to download the IEEE papers, many strict rules are managed due to unauthorized access that may lead to attackers. Hence, registration/membership concepts are included with various criteria.

Application 3:
Some Internet based downloads for premium users and anonymous users restricted by their bandwidth.

3.1 RELATED WORK

***Software Systems* :**
I n software systems, attacks occur due to vulnerabilities in the system or sometimes through virus that was present in the software, where such viruses are named as "man in the middle" unlike the intruder.

***Network Routers*:**
Several attacks can happen due to routing. Therefore, in this concept, attack may occur at the path chosen from where it received or sent fake information.

Many techniques were implemented to detect the selfish attacks in ad hoc network. It was designed for runtime cognitive radio networks to consider the quality of service belonging in CRNs with selfish node coincidence [9]. Their objective is to give

- Least delay
- High throughput
- Efficient delivery ratios

For CR selfish attacks, Chen et al. first identified a threat to spectrum sensing, called (Primary Users) PU emulation attack, in 2008 [17]. In this, a selfish attacker transmits PU signals. This emulated signals make legitimate SUs misunderstand that a PU is active, and so the faked signals obstruct (Secondary Users) SU access to the available spectrum band. Then the selfish SU will pre-occupy the available bands. They detect the faked PU's signals by transmitter verification. Transmitter verification

determines the legitimate source signal by signal energy level combined with the source signal location. Selfish attacks are made by a selfish SU that increases the access probability by decreasing the back of window size in a CSMA based CR network. This selfish attack is a sort of DoS. JaydipSen and KaustavGoswami in 2009 specified an algorithm named as Inference-Based Clustering Algorithm for detection of selfish nodes in wireless mesh networks [8]. This approach used AODV routing protocol. But the method included clustering concept that is time consuming process. In 2014Markov Chain Algorithm and Game Theory Probability, sequence and Accuracy rateGT follow some strategies, but those are not efficient. Markov approach follows the sequence in every time.Minhojo, Longzhe Han, Dohoon Kim and Hoh Peter in 2013 specified reputation method to detect selfish node attacks in Cognitive Radio Ad-Hoc Networks using SU based and calculated the historical selfish behavior data of a node. SnehaThankachan and M.Jebkumari during 2014 announced in enhancing detection rate in Selfish Attack Detection Scheme in Cognitive Radio Ad hoc Networks and conveyed that the distribution reaction mechanism (DRM) technique mainly concentrates on the traffic flow and the signal strength of a particular node and the primary user access time were considered. In 2014, P.V.Niranchana and K.AnishPonYamini reported credit risk value based detection of multiple selfish node attacks in Cognitive Radio Networks with "Credit Risk Value" method which was calculated based upon the total energy of the packets present in the network. Recently again in 2014, SheetalJ.Nagar , Divan G.Raimagia and PinakiA.Ghosh proposed how to identify and eliminate selfish Nodes in Ad hoc Networks. This approach implemented the Watchdog mechanism to identify the attacks in the network. Few parameters like packet delivery ratio, End-to-End delay and throughput were considered here. Continuosly research in detecting selfish nodes had taken place till august 2014 where Suchita S. Potdar and Dr.Malikarjun used Markov Chain and Game Theory technique in this context to detect the selfish attack. Markov Chain Algorithm is used. The game theory method is executed with some strategies but which were not efficient as to markov chain method. The probability is high in every time and hence accuracy rate is lowered andtherefore this method may not be appropriate to be used for longer times.

4. PROPOSED MECHANISM

4.1 Problem Design

In most part of the existing system, selfish attack is detected only partially and some of the approaches were quite complex and managed with minimum routing table structure. Hence, to detect and identify the selfish attacks in Cognitive Radio, it has been assumed that the nodes continuously monitor the forwarding behaviors of their neighbors to determine if their neighbors are misbehaving. To address this problem, behavior based methods with knowledge techniques are proposed as SNAL with considering the following modules to identify selfish nodes in network.

- Module 1: Mobile ad hoc Network Generation using p-p dataset of Stanford University
- Module 2: Communication initiates
- Module 3: Apply Light-Weight Cryptography to set up security

- Module 4: Apply Routing Protocol as “Lightweight Mobile Routing”
- Module 5: Trace out the selfish nodes

4.2 SNAL (Selfish Node Attack Identification using Light weight system)

In Cognitive radio ad hoc networks, selfish attacks are the serious security problem, it can be caused because of the abnormal behavior of the node nothing but the node can be behave like selfishly means that it cannot cooperate with the other nodes in normal manner. [16][15]However the selfish attack can be defining the performance of the network can be degraded because the effected nodes are having poor performance means that they can participate in the transmission of the packets in the network. In this research we proposed new mechanism for anomaly detection technique to detect the selfish nodes in the CR network. In this proposed method follow the new mechanism to find out the selfish node attack in the network that is mainly separated into three parts, the first part is to create the network by using the datasets, second is to encrypt the packet message by using the advanced cryptographic technique namely Lightweight Cryptography and the third part is apply the routing protocol to detect selfish attack. So coming to the first part the dataset shouldcollect the in real time environment, give input to the network to create the nodes of the network. Send the message and apply the encryption mechanism “Lightweight” to encrypt the message of the packets. [5]Finally, Link Reversal Routing protocol is implemented to determine the routing mechanism in the network.Light weight mobile routing algorithm is used to detect the selfish attack. In this context, threshold is considered to act as take the main condition in network, if the attack is detected using the node behavior. If the nodebehaves in normal way there is no attack at all and if in abnormal way then the attack is determined. Dataset is taken from the Stanford University in that Peer-to-Peer network which is the basis as a input to generate the cognitive radio network in a real time environment. This dataset is of very huge size of 113Kb. So basically, only 100 nodes are taken initially and later testing is done for the 113Kb of size.

4.3 Security Measure : Light Weight Cryptography

Lightweight Cryptography is a relatively young scientific sub-field that is located at the intersection of electrical engineering, cryptography and computer science and focuses on new designs, adoptions or efficient implementations of cryptographic primitives and protocols. Due to the harsh cost constraints and a very strong attacker model especially noteworthy is the possibility of physical attacks there is an increasing need for lightweight security solutions that are tailored to the ubiquitous computing paradigm. Every designer of lightweight cryptography has to cope with the trade-off between security, costs, and performance. For block ciphers the key length provides a security-cost trade-off, while the amount of rounds provides a security-performance trade-off and the hardware architecture a cost-performance.

Usually, any two of the three design goals security and low costs, security and performance, or low costs and performance can be easily optimized, whereas it is very difficult to optimize all three design goals at the same time. For example, a secure and high performance hardware implementation can be achieved by a pipelined

architecture which also incorporates many countermeasures against side-channel attacks. The resulting design would have a high area requirement, which correlates with high costs. On the other hand it is possible to design a secure and low-cost hardware implementation with the drawback of limited performance.

Generally speaking, there are three approaches for providing cryptographic primitives for extremely lightweight applications such as passive RFID tags:

(1) Optimized low-cost implementations for standardized and trusted algorithms.
(2) Slightly modify a well investigated and trusted cipher.
(3) Design new ciphers with the goal of having low hardware implementation costs.

In this proposed work, we had minimized the problems in all three approaches. The problem with the first approach is that most modern block ciphers were primarily designed with good software implementation properties in mind, and not necessarily with hardware-friendly properties. This is the right approach for today's block ciphers, because on the one hand the vast majority of algorithms run in software on PCs or embedded devices, and on the other hand silicon area has become so inexpensive that very high performance hardware implementations (achieved through largechip area) are not a problem anymore. However, if the goal is to provide extremely low-cost security on devices where both of those assumptions do not hold, it turns out that many modernblock ciphers do not perform well for these scenarios.

[4][18]The Lightweight Cryptography can be defined as the advanced encryption technique which is one of the very efficient encryption techniques. In this technique, the algorithm follow SP network structure where two operations like substitution and permutation are involved. There are 31 rounds with XOR operation, with block length of 64 bits and key length of 80 bits or 128 bits. The key register is updated in every round. Lightweight Cryptography aims at packet encryption in the cognitive radio network. To accomplish the task, the plain text block is the input of the message. An 80-bit key is XORed to plain text and then the result is passed to S-box layer and P-box layer where later they are merged together. This operation repeats and in each iteration, the key register is updated automatically. Finally, cipher text is generated.

EFFICIENY METRICS

To assess the efficiency of our implementation the following metrics are used:

Area:

Area requirements are usually measured in _m2, but this value depends on the fabricationtechnology and the standard cell library. In order to compare the area requirementsindependently it is common to state the area as gate equivalents [GE]. One GE is equivalentto the area which is required by the two-input NAND gate with the lowest drivingstrength of the appropriate technology. The area in GE is derived by dividing the area inm2 by the area of a two-input NAND gate.

Cycles:
Number of clock cycles to compute and read out the result.
Time:
The required amount of time for a certain operation can be calculated by dividing theamount of cycles by the operating frequency t = cyclesfreq. Throughout this chapter in mostcases100KHz is used as the operating frequency. Therefore in most cases the time isgiven in milli seconds [ms].

Throughput:
The rate at which new output is produced with respect to time. The numberof output bits is divided by the time, i.e. by the needed cycles and multiplied by theoperating frequency. It is expressed in bits per second [bps].

***Efficiency*:**
The throughput to area ratio is used as a measure of hardware efficiency. Thehardware efficiency is calculated by dividing the area requirements by the throughput,i.e.
Efficiency = area /throughput , and is expressed in gate equivalents per bits per second [GEbps].
[]Coppersmith states the following eight criteria as the "only cryptographically relevant" onesfor the S-boxes

- Each S-box has six bits of input and four bits of output.
- No output bit of an S-box should be too close to a linear function of the input bits.
- If we fix the leftmost and rightmost input bits of the S-box and vary the four middle bits, out of reach possible 4-bit output is attained exactly once as the middle input bits range overtheir 16 possibilities.
- If two inputs to an S-box differ in exactly one bit, the outputs must differ in at least twobits.
- If two inputs to an S-box differ in the two middle bits exactly, the outputs must differ inat least two bits.
- If two inputs to an S-box differ in their first two bits and are identical in their last twobits, the two outputs must not be the same.
- For any nonzero 6-bit-difference between inputs, _I, no more than eight of the 32 pairsof inputs exhibiting _I may result in the same output difference _O.
- Minimize the probability that a non-zero input difference to three adjacent S-boxes yielda zero output difference.

This algorithm is more than adequate security for the low-security applications typically required in tag-based deployments, but just as importantly, this matches the design goals of hardware-oriented stream ciphers in the stream project and allows us to make a fairer comparison. Each of the 31 rounds consists of an XOR operation to introduce a round key Ki for $1 < i < 32$, where K32 is used for post-whitening, a linear bitwise permutation and a non-linear substitution layer. The non-linear layer uses a single 4-bit S-box S which is applied 16 times in parallel.

4.4 Selfish Node Attack Detection

Selfish node attack is related to the DoS attacks and man in the middle attacks. In selfish node attack, the node behavior in abnormal way is checked with the normal behavior. This behavior role is included since the node efficiency depends on its behavior only. If a node performs its functions when there is no any infrastructure and if it behaves in a cooperated manner, then communication performance is said to be maximum or else optimal. Any sort of threats like traffic interruptions, interceptions, fabrication leads to selfish attacks. If the packet sending from source to destination by using the routing protocol, if packet is sending to the destination only particular route is present in the network that route can be calculated based upon the routing protocol . The malicious nodes can be defined in this context and thus selfish node area calculated based upon the threshold value of the particular node in these aspects. If the node meets below the threshold then the node is treated as the normal behavior. If the node meets equal or above the threshold then the node is treated as the malicious node and it is considered as possessing selfish behavior.

Step 2: Establishing the paths between the nodes present in the network.A fundamental issue arising in mobile ad-hoc networks (MANETs) is the selection of theoptimal path between any two nodes. A method that has been advocated to improve routingefficiency is to select the most stable path so as to reduce the latency and the overhead due toroute reconstruction. In this work, both the availability and the duration probabilityof a routing path that is subject to link failures caused by node mobility are emphasized. In particular, also focused on the network nodes that move as per to Random Direction model, and derivedboth exact and approximate (but simple) expressions of these probabilities. Through results, the problem of selecting an optimal route in terms of path availability is identified.

Step 3: Apply of routing protocol to estimate the neighboring nodes.

Routing is one of the core problems of networking for delivering data from one node to the other. Wireless ad-hoc networks are also called Mobile ad-hoc multihop networks without predetermined topology or central control. This is because MANETs can be characterized as having a dynamic, multihop, potentially rapid changing topology. The aim of such networks is to provide communication capabilities to areas with limited or no existing communication infrastructures. It uses a peer-to-peer multihop routing instead of a static network infrastructure to provide network connectivity.In a MANET, the router connectivity may change frequently, leading to the multi-hop communication paradigm that can allow communication without the use of BS/AP, and provide alternative connections inside hotspot cells. A dual-mode MS can operate in both the infrastructure and MANET modes using the WLAN interface. A MANET is a type of ad hoc network that can change locations and configure itself on the fly. All nodes in this network are mobile and they use wireless connections to communicate with various networks.

Step 4: Calculate the neighboring nodes by using the distance vector routing algorithm.

Distance-vector routing protocol is one of the two major classes of routing which use the Bellman–Ford algorithm, Ford–Fulkerson algorithm, or DUAL FSM (in the case of Systems' protocols) to calculate paths.A distance-vector routing protocol requires

that a router informs its neighbors of topology changes periodically. Compared to link-state protocols, which require a router to inform all the nodes in a network of topology changes, distance-vector routing protocols have less computational complexity and message overhead.The term "distance vector" refers to the fact that the protocol manipulates vectors (arrays) of distances to other nodes in the network. The vector distance algorithm was the original ARPANET routing algorithm and was also used in the internet under the name of RIP (Routing Information Protocol).
Step 5 : Estimate the node cost using the Heuristic ranking algorithm.
In computer science, heuristics are techniques designed for problem solving quickly when classic methods are too slow, or for finding an approximate solution when classic methods fail to find any exact solution. Heuristics may produce results by themselves, or they may be used in conjunction with optimization algorithms to improve their efficiency (e.g., they may be used to generate good seed values).Results about NP-hardness in theoretical computer science make heuristics the only viable option for a variety of complex optimization problems that need to be routinely solved in real-world applications.
Step 6: Find out the threshold value of each node in the network.
Satisfiabilityof Boolean formulas is a problem universally believed to be hard. Determining the source of this hardnesswill lead, as is often stressed, to applications in domains even outside the realm of mathematics or computer science;moreover, and perhaps more importantly, it will enhance our understanding of the foundations of computing.In the beginning of the 90s, several groups of experimentalists chose to examine the source of this hardness from thefollowing viewpoint: consider a random 3-CNF formula with a given clauses-to-variables ratio, which is known as the densityof the formula. What is the probability of it being satisfied and how does this probability depend on the density Theirsimulation results led to the conclusion that, if the density is fixed and below a number approximately equal to 4:27, thenfor large n a randomly chosen formula is almost always satisfiable; whereas if the density is fixed and above 4:27, a randomlychosen formula is, for large n, almost always unsatisfiable. More importantly, around the complexity of several well-known complete algorithms for checking satisfiability reaches a steep peak

LINK REVERSAL ROUTING PROTOCOL

Node communication in the network is understood by routing structure. Routing protocol thus plays a crucial role in any type of communication system. In this task, Link Reversal Routing Protocol (LRR) is chosen for implementation. This protocol is focused with three types of algorithms:

- GafniiBertsekas (GB)
- Lightweight Mobile Routing (LMR)
- Temporally Ordered Routing Algorithm (TORA) .

The algorithm "Lightweight mobile algorithm(LMR)" is more stable compare to the other algorithms in the protocol. The method contains two phases : routes establishment and routes maintenance. The LMR is free of loop and dead lock

structures in the network. It has firm route establishment in between the nodes for communication. It can be worked even in the network when partitioned. The implementation of the method is portioned in three phases :

- Route Construction phase - routes are built in particular manner based upon the cost and the distance of the particular nodes present in the network.
- Maintenance phase – in this phase, the route changes can happen in the network because of the dynamic topology. Further, if any new nodes are added, the topology may change. So routing needs to be updated.
- Destruction phase - in this phase, the routes can be disconnected if the nodes no longer reside in the network.

In some situations the maintenance phase can take the work of the deletion of the routes which are not used in longer time. That means the third phase is the optional phase in the algorithm where it can be used or not used in the process. Adjacent nodes of node i, can be denoted as Ni. For each adjacent node j, there can exists a link li,j between the node I and node j, li,j may be undirected or the directed. Lightweight mobile routing algorithm uses three types of control packets.

- QRY(Query), this packet contains of Source node ID, destination node ID, a sequence counter and transmitting node ID.
- RPY(Reply), this packet also contains the same of the query packet.
- FQ(Failure Query), in this packet contains the destination node ID and transmitting node ID.

This protocol can be used to establish a route between the nodes of the mobile radio network to communicate with the intermediate channels. The packet of the message can be transmitted only when the particular route is present in the network. The necessary routes are described with the help of the routing protocol and detection of attack can also be done using the routing protocol.

5. EVALUATION AND RESULTS

Results and observations are presented with the implementation of the proposed work ie to find out selfish node attacks. Total process is categorized into five modules. Firstly, collected the dataset in real time environment to generate CR network. Then packets are sent using the nodes path. Third, apply of light weight cryptography for the encryption purpose that means to encrypt message of the packet. Next, implemented routing protocol namely lightweight mobile routing algorithm in the link reversal routing protocol. Lastly, traced out the selfish node attack by using the entropy of the threshold value

As required to upload the data set values in the database for the network creation. Built the network by using the real time dataset that can be collected by the Stanford university. The name of the data set can be Peer-to-Peer dataset in that the values presented namely To node, From node, cost and Threshold value.

Each node can consists of the neighboring nodes in the network that means which nodes are adjacent to that node can be called neighbor nodes. We can send the

information to the adjacent nodes in that network. For example in the above diagram shows the neighboring nodes of the node 1 can be visible.

The below figure says that the node in the network can perform the above activities . In the broadcast of the particular node can construct the path from one node to the other node , those nodes are neighbors of particular nodes . This can shows the which nodes are neighbors of particular node ,construct path to that nodes and send the message to that nodes can defiantly establishing path.

This figure says that the Routing Protocol concept . In this take the node number 3 and give the all possible paths to the remaining other nodes . It shows the five paths , if tha packet is send to othernodes . The destination node 2. The Get List may represents the paths of particular nodes . The Send option can be used for sending the message of particular node.

It also shows the selected path which is shortest to the sending node and the receiving node . The path is established by using the Lightweight mobile Routing (LMR) Algorithm. This the type of the Link Reversal Routing Protocol . Establishing path in the reverse format .mentioned in the Routing protocol concept

Thisshows the clear picture of the attacks, which nodes are behave selfishly in the mobile ad hoc networks. The malicious nodes are detected based upon the threshold value of the particular node. The entropy can be taken as threshold. Selfish Node Attack is the one of the type of Selfish Attacks. So these nodes are misbehaving nodes.

In the above Figure, the ratio should be shown in between the selfish (malicious) and the normal nodes . Let first take the >25 nodes find out the selfish nodes , after >50 nodes again find out the selfish nodes until >100 nodes find out the selfish nodes based upon the entropy of the threshold value of particular nodes presented in the network . In this diagram the blue color points may represents the normal nodes and the red color points can represents the number of selfish nodes occur in that network.

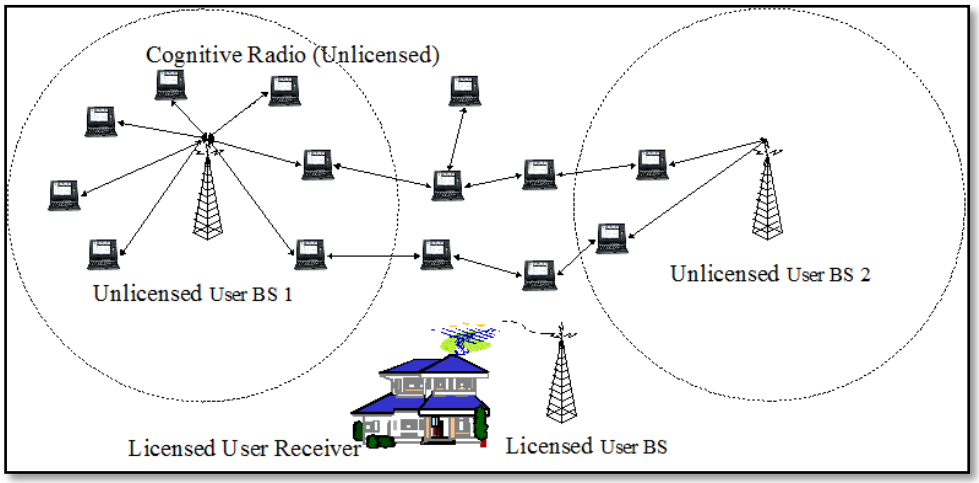


Fig1: Cognitive Radio Scenario

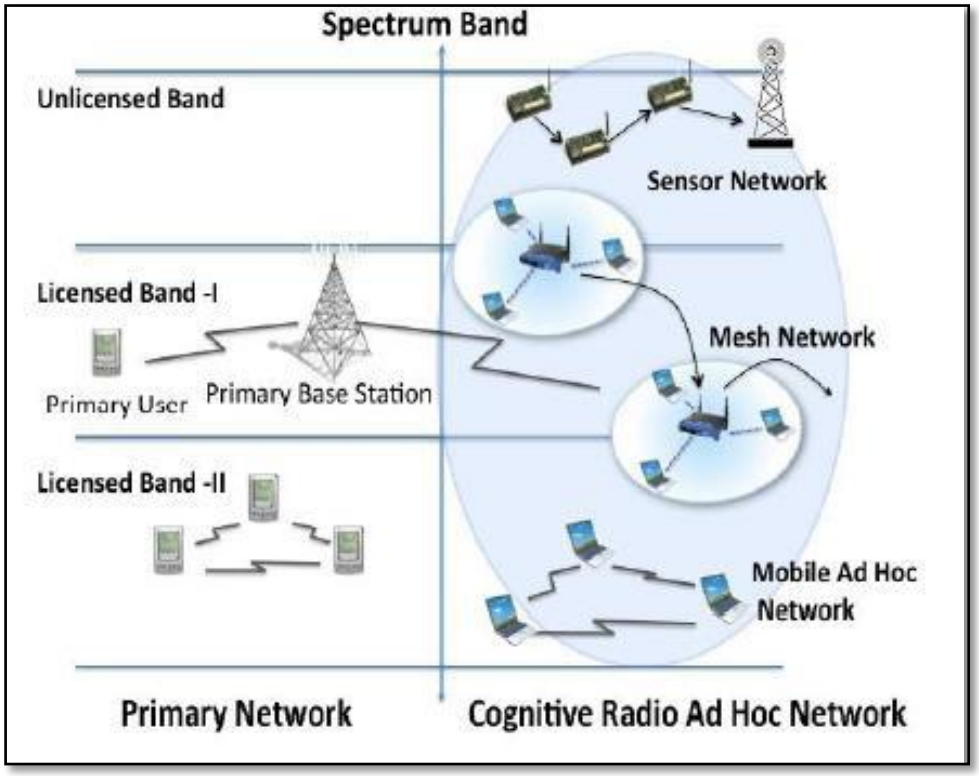


Fig 2: Spectrum allocation in CR networks

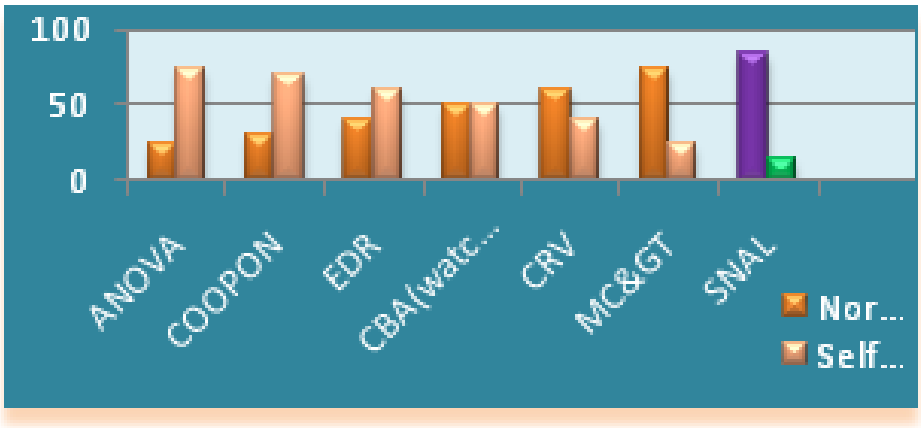


Fig 3: Comparison study of proposed SNAL Method with existing work from 2009 to 2014

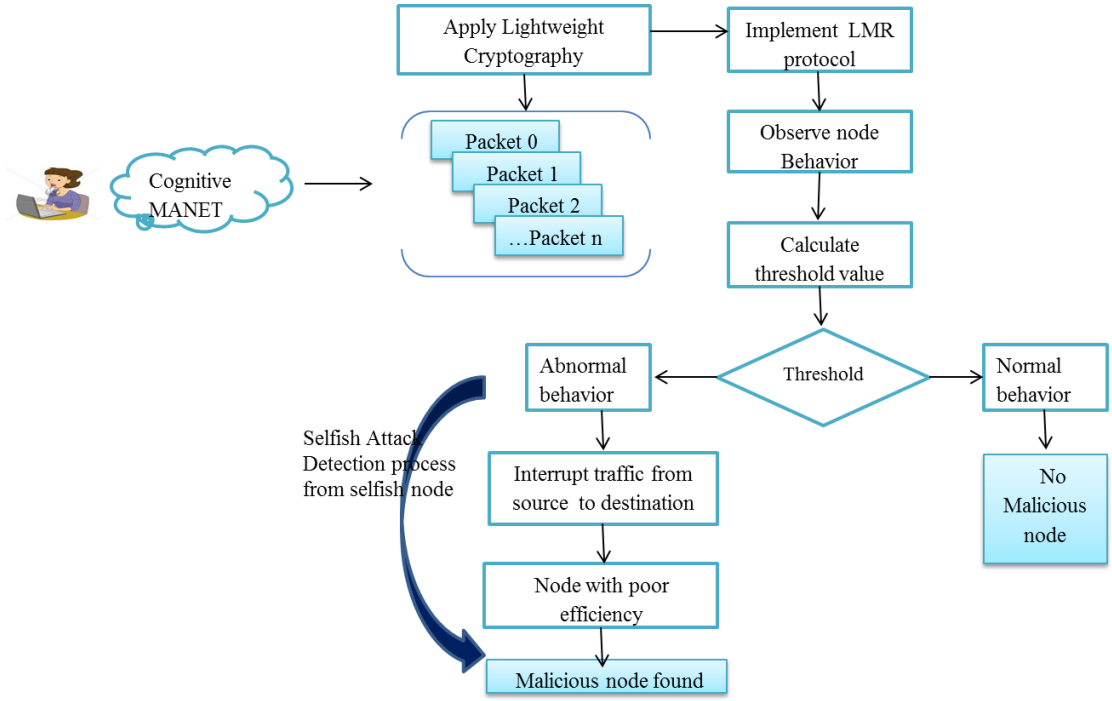


Fig 4: Proposed SNAL(Selfish Node Attack Identification using light weight system)

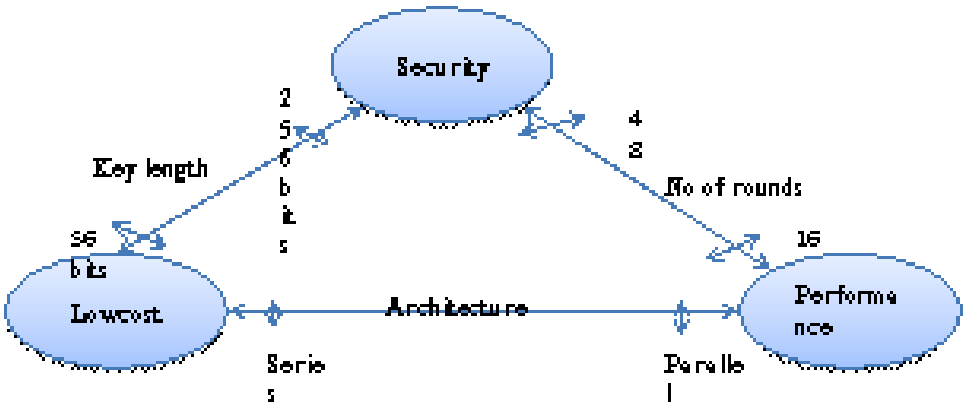


Fig5: Security in Light weight encryption

ENCRYPTION

Step 1 : Take input as plain text .
Step 2 : Add plain text with Register key value.

```
generateRoundKeys()
fori =1 to 31 do
        addRoundKey(STATE,Ki)
        sBoxLayer(STATE)
        pLayer(STATE)
end for
addRoundKey(STATE,K32)
```

Step 3 :Add Round key with the plain text.
Step 4 : Update the KeyRegister in each and every time until the number of 31 rounds completed
Step 5 : Calculate the values of the sBoxLayer and pLayer based upon the substitution and the permutation values by using the Boolean functions of the variables.
Step 6 : Finally at the last round can get the cipher text of the message.

Fig 6: Encryption scheme

DECRYPTION

Step 1 : Take input as cipher text .
Step 2 : Add cipher text with Register key value.

```
generateRoundKeys()
addRoundKey(STATE,K32)
fori =31 down 1 do
        invPLayer(STATE)
        invSBoxLayer(STATE)
        addRoundKey(STATE,Ki)
end for
```

Step 3 :Add Round key with the cipher text
Step 4 : Update the KeyRegister in each and every time until the number of 31 rounds completed.
Step 5 : Calculate the values of the sBoxLayer and pLayer based upon the substitution and the permutation values by using the Boolean functions of the variables.
Step 6:Finally at the last round can get the plain text of the message.

Fig 7: Decryption scheme

Step 1 : Collect the real time dataset (Sender node, Receiving node, cost, port number) for the creation of Cognitive radio ad hoc network .

Step 2: Establishing the paths between the nodes present in the network.

Step 3: Apply the routing protocol estimate the paths which are the neighboring to that source node.

Step 4: Calculate the neighboring nodes by using the distance vector routing algorithm.

Step 5 : Estimate the cost of the nodes using the Heuristic ranking algorithm.

Step 6: Find out the threshold value of each node in the network.

Step 7: The threshold value can be calculated based upon the distance and the cost of particular node present in the tree.

Step 8: Compare the value with the default threshold value .

Step 9: If the node value is less than the default threshold value then that node can be considered as the normal node .

Step 10: If the node value exceed the default threshold value then that node will be detected as the malicious or selfish node

Fig8: Simplified steps in proposed method

A sequence of snapshots of the Gnutella peer-to-peer file sharing network is considered. There are total of 9 snapshots of Gnutella network collected in August 2009. Nodes represent hosts in the Gnutella network topology and edges represent connections between the Gnutella hosts.

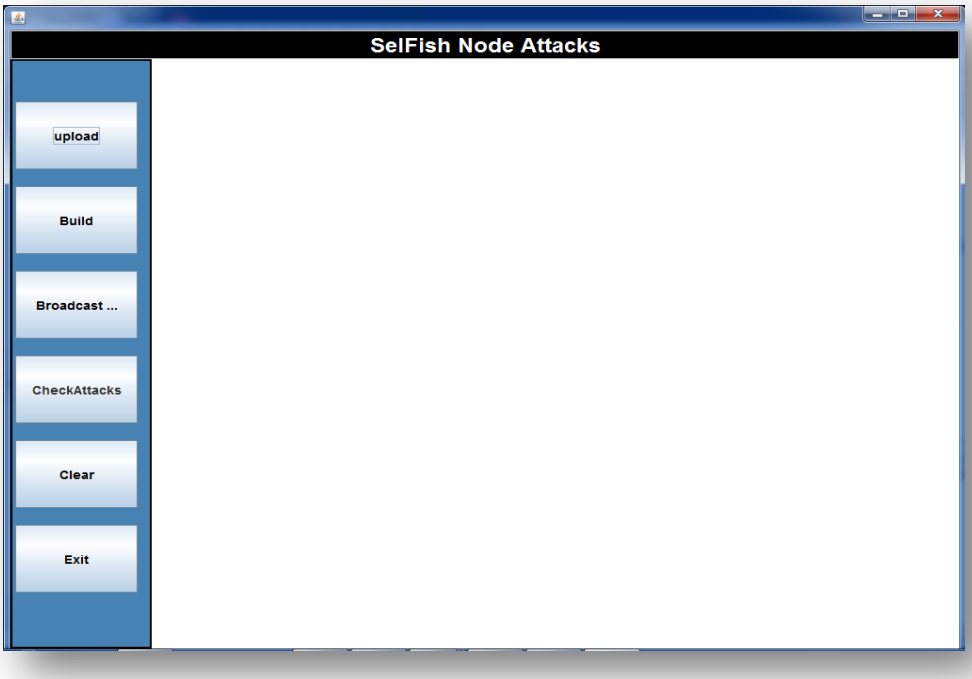
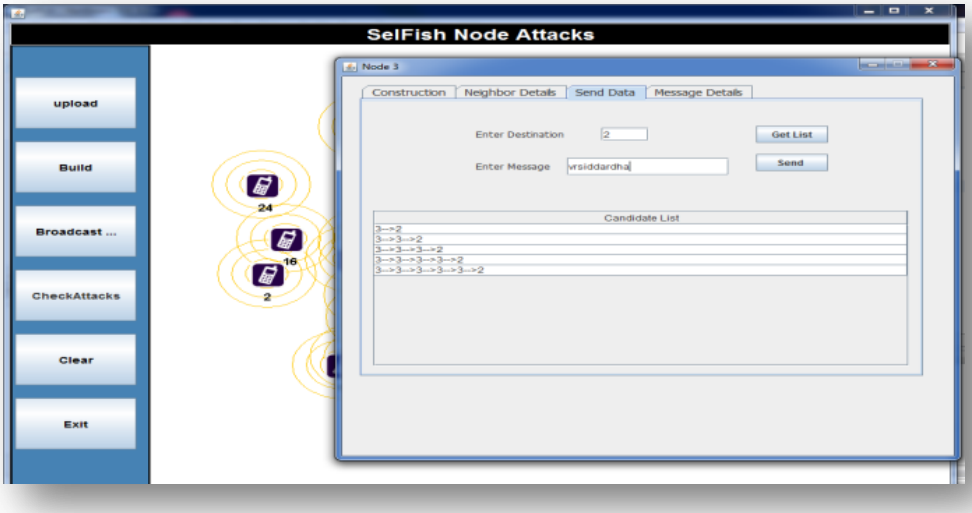


Fig9: Home page of proposed technique "SNAL"



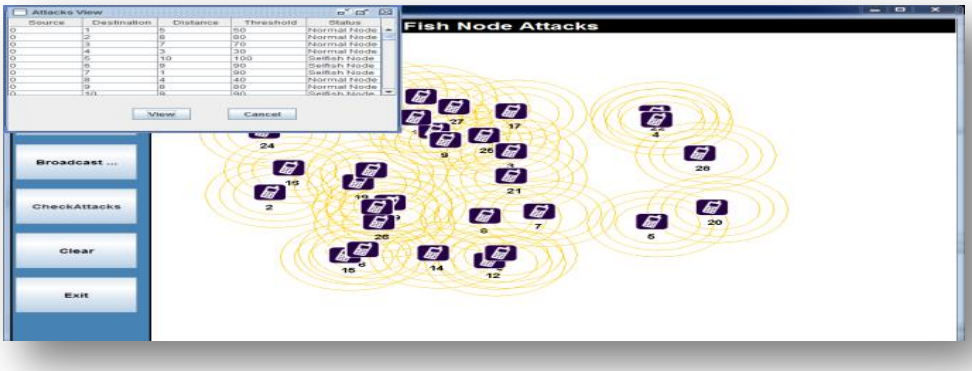


Fig 10: Implementation of LMR

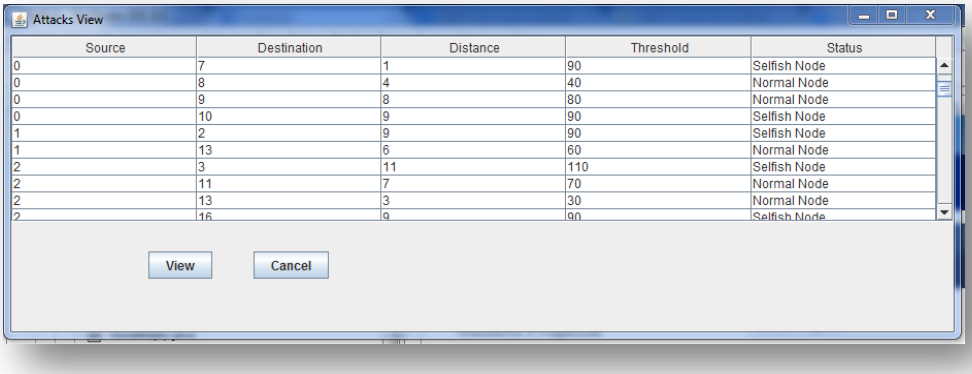


Fig11: Neighboring nodes

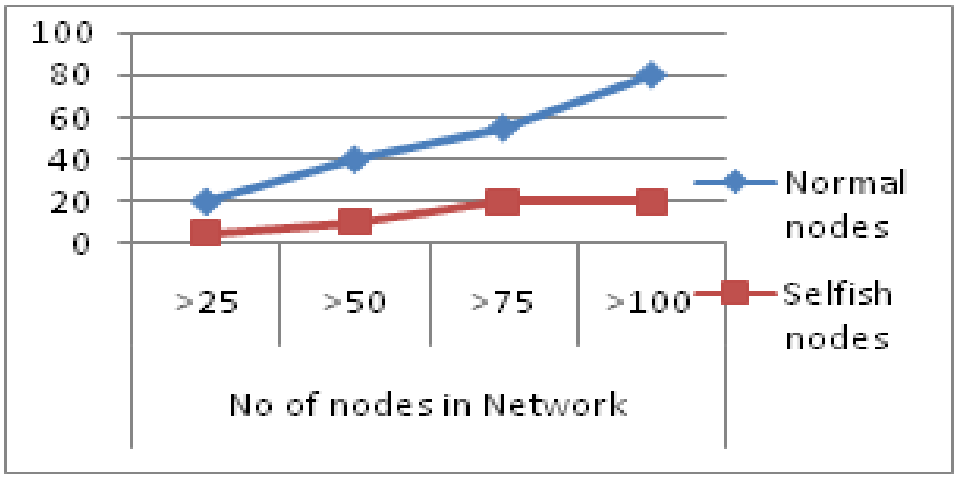


Fig12: Selfish nodes identification

Table 1: Peer to Peer dataset of Stanford University

Datasetstatistics	
Nodes	62586
Edges	147892
Nodes in largest WCC	62561 (1.000)
Edges in largest WCC	147878 (1.000)
Nodes in largest SCC	14149 (0.226)
Edges in largest SCC	50916 (0.344)
Averageclustering coefficient	0.0055
Number of triangles	2024
Fraction of closed triangles	0.001294
Diameter (longestshortestpath)	11
90-percentile effective diameter	6.7

6. CONCLUSION

Cognitive radio ad hoc network has been recently attracted many researchers based upon their interest. In this network, security has given much importance due to network problems raised from attacks. Selfish attacks are one of the dangerous security issues that need to be addressed since it decreases the performance of a communication system with thepresence of selfish devices. An effective schema called as "SNAL (Selfish Node Attack using Lightweight)" is used to detect selfish attacks namely selfish node attack in Cognitive ad hoc networks. Modern technology implemented using Net beans is adopted. Hence, a single approach is proposed and successful to detect attacks. This was found at the time of the packets in transmission. Packets were encrypted by using the encryption mechanism of lightweightcryptography and the paths arechosen by using light-weight mobile routing protocol in link reversal routing. In this regard, future work can be extended to study & make necessary precautions by including some prevention methods that can deal to reduce the value of the threshold and increase the genuine nodes with the adequate measures.

7. REFERENCES

[1] http://en.wikipedia.org/wiki/Selfish attack.
[2] http://link.springer.com/chapter/10.1007%2F978-1-4020-8737-0_87#page-1

[3] J.Junge, B.Krishnammurthy, and M.Rabinovich"Selfish attacks in MANETs Characterization and Implications for CDNs and websites",Proc.11thInt'lConf.(WWW),pp.252-262,2002.

[4] M. Bhailey, E. Cookes, F. Jahanianh, "A Survey of communication Technology and Defenses," Proc.Cyber security Applications and Technology Conf. for Homeland Security, pp.299-304,2010.

[5] C.Y. Chyo and J. Caballerao, Insightsfrom the Inside: A View of Lightweight routing protocol," Proc. Third USENIX Conf. Large-Scale Exploits and Emergent Threats: Selfish attacks and Man in the middle attack, pp.1-8, 2012.

[6] V.L.L. Thingkhanomn, M. Sloman king, and N. Dulaye, "A Survey of selfish node attackof Service Attacks," Proc. SEC, pp. 229-240, 2009.

[7] B. Stonye-Gross, M. Covsa, L. Cavallaruo, B. Gilberit, M. Szydlowkski, R. Kemmyerer, C.

[8] Kruegel, and G. Vigna, "Intrusion Detection system in the selfish attacks in MANET," Proc.ACM Conf. Computer Comm. Security, pp.635-647,2012.

[9] N. Ianelli and A. HackwoKrth, "Lightweight routing protocol for the mobile routing algorithm," Proc. 18th Ann.FirstConf., 2008.

[10] T. Haolz, M. Steinerr, F. Dahl, E. Biersack, and F.C. Freiling, "Measurements of the Packets delivery at the router and efficiency of the Router," Proc.FirstUsenixWorkshop Large-Scale Exploits and Emergent Threats (LEET), 2009.

[11] A. Schaerrer, N. Larrieeu, P. Owezsarski, P. Borgnatt, and P. Aabry, "Lightweight mobile Routing protocol in the Mobile networks," IEEE Trans.Dependable Secure Computing, vol. 4, no. 1, pp. 56-70, Jan.-Mar. 2009.

[12] Y. Tevfik and A. H¨useyin, "A survey of spectrum sensing algorithms for cognitive radio applications," in IEEE Communications Surveys & Tutorials, 2009, pp. vol.11, pp. 116-130.

[13] Carlos CordeiroChittabrataGhosh, "Markov Chain Existence and Hidden Markov," in IEEE Conference, 2009, pp. 1-6.

[14] J. G. Kim, and D. Lee C.-H. Chin, "Stability of Slotted Aloha with Selfish Users under Delay Constraint," in KSII Trans. Internet and Info. Systems, March 2011, pp. vol. 5, no. 3,542–59.

[15] Douglas Sicker, Gary Minden, DipankarRaychaudhuri Peter Steenkiste, "Future Directions in Cognitive Radio Network Research," NSF Workshop June 2009.

[16] Z. Gao et al, "Security and Privacy of Collaborative Spectrum Sensing in Cognitive Radio Networks," in IEEE Wireless Communication, 2012, pp. vol. 19, no. 6,106–12.

[17] S. Li et al, "Location Privacy Preservation in Collaborative Spectrum Sensing," in IEEE INFOCOM, 2012, pp. 729–37.

[18] Alexander Wong, Pin-han Ho Xiao Yu Wang, "Dynamic Markov-Chain Monte Carlo Channel Negotiation for Cognitive Radio," in IEEE INFOCOM 2010, canada, 2010.J. Leskovec,