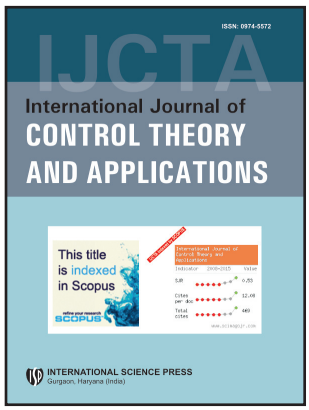


International Journal of Control Theory and Applications

ISSN : 0974-5572



Volume 10 • Number 24 • 2017

# Performance Analysis and Design of Automatic Attack Identification for Ad-Hoc Wireless Channel and Improvement in Coverage

**Savita Patil[a] and A.M. Bhavikatti[b]**

[a]*Research Scholar, VTU RRC, Belagavi. Email: sampatil949@gmail.com*
[b]*Professor & HOD of CSE, BKIT, Bhalki. Email: arvindbhavikatti@gmail.com*

***Abstract:*** In conventional cellular networks suffering with an irregular installation of high power consumption base stations, where users can be established communication through the hop and multiple hopes for data transmission. The existing networks are irregular deployment, due to security less and low channel capacity, the attacks and interferences are more. The heterogeneous soft reservation multiple accesses (HSRMA) with priority assessment (PA) networks is proposed and it is a category of contention based Ad hoc wireless network for better coverage of nodes in a high traffic load. The HSRMA with PA, the stage of proposed work is to create new large nodes in a network for high coverage and to avoid the attacks. The created network divided into clusters of the all nodes and each cluster has a winner to look after neighborhood nodes and to minimize the distance from winner to neighborhood node. This minimized distance can be utilized for other nodes for data transmission, so the bandwidth is reduced and thereby enhancing the coverage area capacity. Second stage of the proposed work is to deployment of base station with small-cell in existing technology of macro-cellular networks referred to as Heterogeneous Networks. A Heterogeneous Network consists of Macro-Cellular base station and underlying Small-Cell base station used in LTE or WiFi technologies to increase network capacity and better coverage. Finally, the proposed work is analyzed in terms of numerical studies and simulations are conducted to validate the analysis in MATLAB 2014A.

***Keywords:*** Ad-HOC Wireless Network, HSRMA, Macro, Channel Capacity, Converge area.

## 1. INTRODUCTION

In Efficient data Transmission, Secure and Efficient data Transmission protocol for cluster-based WSNs. The Identity-Based Online/Offline digital Signature (IBOOS) protocol is designed with the same purpose and scenarios for CWSNs with higher efficiency. The efficient data Transmission IBOOS operates similarly to the previous SETIBS, which has a protocol initialization prior to the network deployment and operates in rounds during communication. We first introduce the protocol initialization, and then describe the key management of the protocol by using the IBOOS scheme, and the protocol operations afterwards [25]. Key management for security module, security is based on the DLP in the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. The IBOOS scheme in the proposed

SET-IBOOS consists of following four operations, extraction, offline signing, online signing and verifications. The Key management module, the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security. Neighborhood authentication module, used for secure access and data transmission to nearby sensor nodes, by authenticating with each other. Here, "limited" means the probability of neighborhood authentication, where only the nodes with the shared pairwise key can authenticate each other. Storage cost module, represents the requirement of the security keys stored in sensor node's memory. Network scalability, indicates whether a security protocol is able to scale without compromising the security requirements. Here, "comparative low" means that, compared with SET-IBS and SET-IBOOS, in the secure data transmission with a symmetric key management, the larger network scale increases, the more orphan nodes appear in the network. Communication overhead module, the security overhead in the data packets during communication. The Computational overhead module, the energy cost and computation efficiency on the generation and verifications of the certificates or signatures for security. The Attack resilience module, the types of attacks that security protocol can protect against.

The demand in the wireless network and to meet the customer requirements in the heterogeneous wireless network, the ad hoc relay nodes concepts has been introduced for WLANs to enhance the transmission of the data capacity and also network converge area improvement. The proposed technology for WLAN muti-hop ad hoc is mixed of network capacity, identification of users, security and to provide the quality of service [1].

In the mobile wireless communication still the research have been continuing to maintain connection establishment between network and user, to increase the network capacity, to reduce the delay and for throughput improvement the heterogeneous for mobility protocol is selected. The proposed techniques is to provide the more security and enhancement of effectiveness for the identification of attacks in the network [2, 13,14].

In [3] the authors are proposed investigation of muti-cell MIMO with VBLAST/STBC system performance for the DL transmission and STBE processing for UL transmission. The precoding techniques are used for enhancement of network capacity by comparing with IP and without IP. It is found that, the proposed network has supported with multiple users without comprising the performance level [12]. The system has interference is better than in the noise limited scenario because of dominant noise in the network. Moreover, it is inferred that ICSI can considerably degrade the system performance due to eigenvalue perturbation. In the context of multi-cell MIMO systems, it is further observed that SVD aided MUTP outperforms other precoding techniques by mitigating MSI and CCI. Throughout this article, we have made an idealistic assumption of perfect synchronization among the BSs. Our future study will focus on the assessment of the system performance under imperfect synchronization between BSs and network latency [3, 15].

The MHCNs capacity has been analyzed, where the outmoded macro-cells, low power base stations are assigned and where the base station data is transmitted to destinations through one hop or multi hop are supported [11, 17]. The data transmission from one user to another user based on the frequency bands that provide the independent homogeneous PPPs for the mobiles users. The proposed MHCNs is a better technique in terms of capacity enhancement and SINR. The increasing the capacity due to splitting of the cell into macro-cells and it is enhances the transmitting power. This system is avoids the cancellation and extended cooperation of MIMO communications [4, 16].

The HetNet network mainly concentrated on victim of users, that analyzed the various interferences techniques that are based on the inter cell and macro cell interference coordination. The author has concluded that picocell is the best technique to optimize the user's victim [9]. The proposed system is best suited for the poor signal quality which is associated with macro cells. It provides the very best quality of service to the macro cells satisfies the users and to avoid the macro cell coverage problems between the neighboring picocells and it also utility to add to the corresponding bit rates to the users [5, 18].

In [6, 10] the authors are proposes the resources allocation problem to solve the CR based femtocells network that makes the network channel imperfect spectrum sensing and uncertainty in the real time communication scenario. Mainly, while interfacing with each MU, the sum rate of all FUs are kept at minimum threshold to optimize the various channel constraints and to remove the unsatisfying numeral problems the sub channel allocation concept has been adapted in the proposed work. For optimization of power distribution, the fast barrier method is used and to trickle the network constraints the Bernstein approximation is used and these two techniques are optimized the capacity gain and fast coverage of network [17, 20].

The almost blank subframes scheme which is basically a genetic method for elimination of the interference in the network [8]. This method is the adapted for the bandwidth sharing by including the macrocell and picocell concepts and it can find the base stations without comprising the resources utilization. The almost blank subframes system uses the macro user equipment system for high throughput, range expanded for user equipment, delay, packet loss error and interference [7, 18].

## 2. METHODOLOGY

In this paper, we evaluate two heterogeneous systems incorporating WiFi and VLC. Our goal is to provide a proof of concept for the coexistence between these two communication bands. Within a short distance between the transmitter and the receiver, the hybrid VLC could perform much better than the WiFi system in the crowded wireless environment. As a complementary technique, VLC deserves further investigation. However, on the one hand, WiFi infrastructures are prevalent and highly acceptable by most consumers; on the other hand, WiFi may outperform VLC in the case of long-distance data transmission or the existence of obstacles. We have also proven through theoretical analysis that the aggregated system is capable of providing better network performance than that of the no aggregated system for most delay-sensitive applications. Therefore, we conclude that the aggregation between WiFi and VLC is worthy of further study, to effectively utilize the aggregated bandwidth and to lower the network delay [19]. In created network, the first node is responsible for generation of global control signals or settings of the spontaneous network like session key and user id's. Each node should be configuring its own data IP, data security and user data, using this information any node can be part of the network. If any node shares the same information to any other node, it will change to ideal mode.

The spontaneous wireless Ad Hoc networks creation is high secured with self-configuration protocol and it is able to generate the network nodes and secure services without any fixed infrastructure. In the proposed work the network creation stages, communication between the nodes, data sharing and management of network are explained. In the proposed work, considered a one tier heterogeneous Ad hoc wireless network model which consists of 25 nodes, each node associated with the HSRMA. Let $N_i$ denote the number of user elements (UE) called femtocells and the area which consists the number nodes is called region of area (RoA). The RoA consists of randomly distributed high traffic loads and their locations. Each UE deployed at the center of neighborhood nodes. The users are either assigned to particular node with probability of '$p$' and other user having probability of 1-$p$. In the created network, each UE is surrounded on location origin ($x$, $y$) and each with its own $p$.

UE's available at the network area of HSRMA and faces higher interference by considering the both macro and femto cells. Finally orthogonal frequency division multiple access (OFDM) and round robin scheduling are applied to reduce interference and identification of attacks. Signal to interference and noise ratio (SINR) is a function of signal strength of availability like path loss, thermal noise and bandwidth sharing.

**At transmitter node:** SINR of transmitter of FSRMA by a US, $i$ associated with base station $j$, the almost block sub frame (ABS) of each UE represents as:

$$UE_{i,j}^{ABS} = \frac{UP_t^j x CG_i^j}{UP_t^k x CG_i^k + {}_i^2} \quad (1)$$

where, UP is power consumed by user transmitter and CG is channel gain coefficient from the base station.

$UP_t^k$ is interfering base station of $k$ and $\sigma_i^2$ is thermal noise of UE $i$

**At receiver node:** SINR received by a UE $i$ associated with base station $j$ scheduled decreasing ABS sub frames and receiving interference free signal will be

$$R_{i,j}^{ABS} = \begin{cases} \dfrac{UP_t^j x CG_i^j}{\sum_{k \in \cap_p, k \neq j} UP_t^k x CG_i^k + \sigma_i^2} & \text{if } j \in_p \\ \dfrac{UP_t^j x CG_i^j}{\sigma_i^2} & \text{if } j = M \end{cases} \quad (2)$$

The received bit rate is most important and the expected bit rate to be received by a user is depends upon the SINR receiver and also depends on bandwidth available at the target base station. Based on the number of users allocated with its target base station, the received bit rate various, therefore the receiver user bit rate is inversely proportional to the base station allocation users. So the following various cell allocation techniques are discussed.

**Received power with reference signal (RPRS):** Since the number UE's are associated with a base station, the transmit power difference between pico and femto cells and base stations are reduces in fairness. Using RPRS, the UE $i$ gets allocated with station $j$ if

$$\text{Serving Id}_i = \text{Arg}_j \{RPRS_{i,j}\}$$

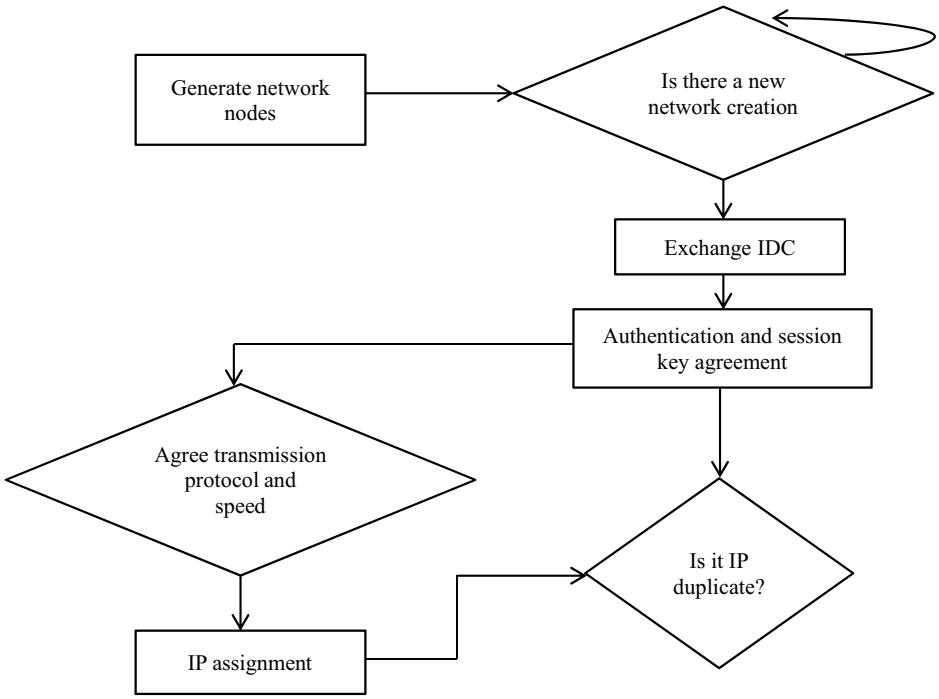


**Figure 1: Proposed flow diagram of network creation and nodes ID and IP assignment**

**RPRS and Bias:** Cell bias (λ) added to RPRS is well suitable to improve offload at user element and utilization of resources in small cells as shown in eq (3)

$$\text{Serving Id}_i = \arg_j \max\{\text{RPRS}_{i,j} + \lambda_j\} \tag{3}$$

In the created network any first node creates the spontaneous network with number of nodes 26 and each node has a randomly generated session key for authentic and these keys are exchanged between any two nodes after the verification phase. Figure 1. shows the nodes joining in the network, node authorization, authentication, transmission protocol, speed, IP address, routing and agreement on session key. Suppose node B wants to join an existing network say node A, it must choose a node within network range to verification of sessions. Node A will send its own public key to B to send its IDC signed by A's public key. After exchanging of secrete keys by both of them, then network is validated to exchange the information data between them.

The following table shows the network setup and it includes base station density, network path-loss exponent, normal logarithmic parameters formation, incorporates network model parameters declaration, noise parameters declaration, SINR threshold, coverage numbers, analytic or integration numbers and radius of disk region.

**Table 1**
**Proposed network setup parameters**

| | |
|---|---|
| Base station density | 0.2887/2 |
| Network path-loss exponent | 3.8 |
| Normal logarithmic parameters formation | $\sigma = \frac{\sigma_{db}}{10\log_{10}10}$, where $\sigma_{db} = 10$ |
| Incorporates network model (a) | $\alpha = \frac{*\pi\beta}{k^2}$, where $\beta = e^{\frac{(2-3.8)}{\beta^2}\times\sigma^2}$ and $k = 6910$ |
| Noise parameters (N, P and W) | $N = \frac{10^{\left(\frac{-96}{10}\right)}}{1000}$, $P = \frac{10^{\left(\frac{62.2}{10}\right)}}{1000}$ and $W = N/P$ |
| SINR threshold in dB | $\text{SINR} = \frac{10^{t \text{ value in dB}}}{10}$, where $t$ value = −10 to 25 |
| Coverage number | 1 |
| Analytic or integration numbers | $10^3$ |
| Radius of disk region | 20 |
| Number of simulations | $10^4$ |

**Algorithm 1:** Attacks detection and localization

**Phase 1:** Using FSRMA, the unique ID for all network nodes are generated by declaring number of nodes, round trip and time

**Phase 2:** Define the number of clusters and its nodes in the network

**Phase 3:** Assume $N_c$ is the network cluster

**Phase 4:** For($i = 0$; $i <= N_c$)

{

Attacker Node N = 0;

Functioning of attack detection by verifying the each node ID in every cluster

$N = N^{++}$;

}

**Phase 5:** Perform the detection in every cluster

**Phase 6:** Identify the number of attacks in N

**Phase 7:** Identify the attacker by verifying the their (X,Y) coordinate values of position

**Phase 8:** Display the number of attacks and their positions

The algorithm 1 has eight phases to find the attacks and their position, the 25 nodes are divided into three different regions and for each region, and representer is identified as shown in Figure 2.

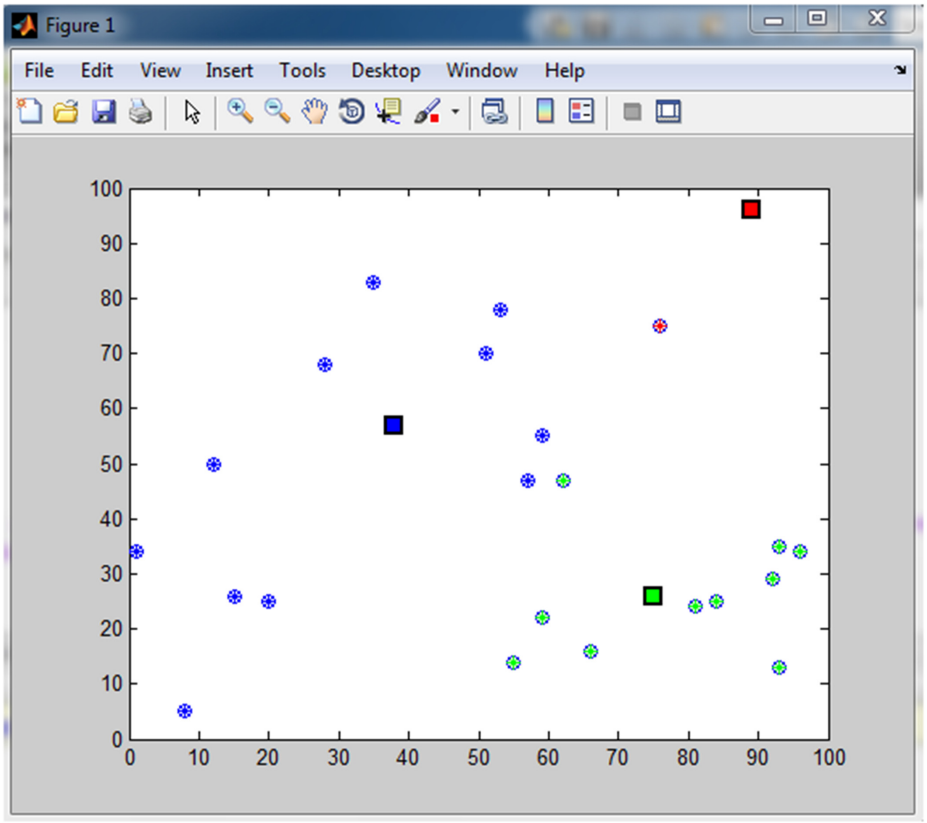


**Figure 2: Nodes creation, division of region and identification of representer**

To identify the attacks, the partitioning Around Medoids (PAM) algorithm is used to achieve high efficacy and clustering analysis. The PAM detects the statistical attacks in normal attack and the same node is partitioned into two clusters based on distance between two Medoids $D_m$ and it is given by $D_m = ||M_i - M_j||$, where $M_i$ and $M_j$ are the Medoids of two clusters. For without attacks condition, the $D_m$ is small and under the attacks condition $D_m$ will be larger.

## 3. RESULTS AND DISCUSSION

The simulation is performed under window 7 environment on MATLAB 2014a. Let us consider the number of nodes deployed in the simulation window for e.g. 3000X3000. The nodes are deployed in 2D platform. Each and every position of nodes are defined, thus from the initialized value, the attackers location in the 2D area can be

determined accurately. The complete design, Graphical User Interface (GUI) has been created which includes the network initialization, clustering and attacks location identification as shown in Figure 3. The attacks locations are 13, 63, 71 and 95 with respective to *x*-axis and these attacks identifications are based the representer in network region as mentioned in the Figure 3.

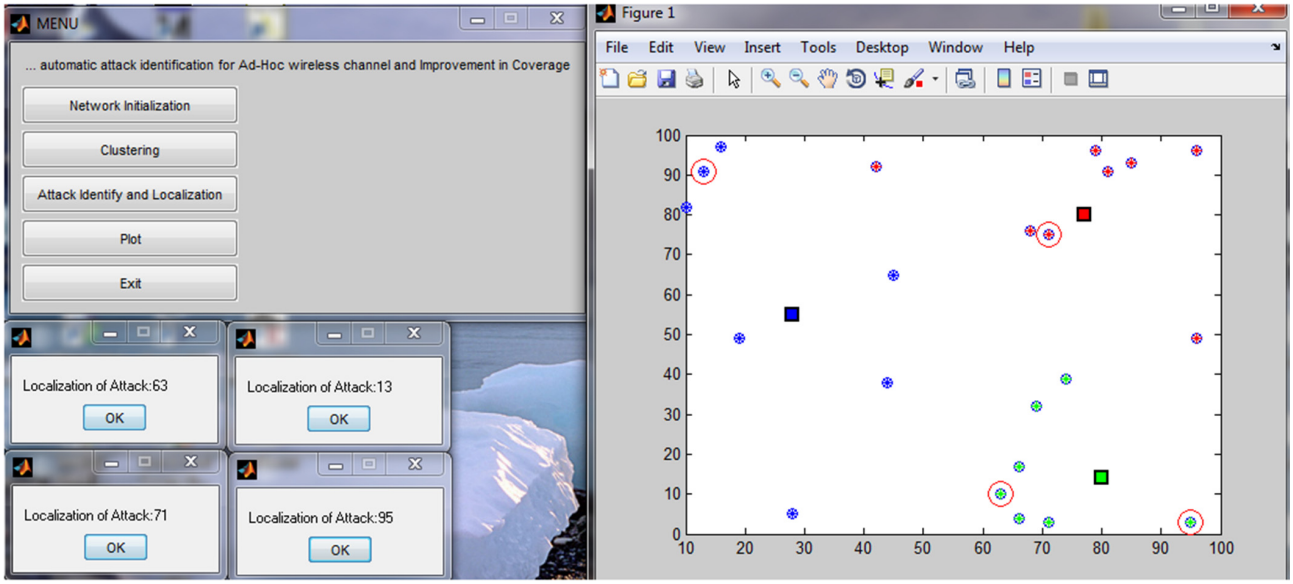


**Figure 3: Nodes creation, division of region, identification of representer and location of attacks**

If a spoofing attacker sends packets at a different transmission power level from the original node, based on our cluster analysis there will be two distinct RSS clusters in signal space (i.e., Dm will be large). We varied transmission power for an attacker from 30 mW (15 dBm) to 1 mW (0 dBm). We found that in all cases Dm is larger than normal conditions. Figure 5b presents an example of the Cumulative Distribution Function of the Dm for the 802.11 network when the spoofing attacker used transmission power of 10 dB to send packets, where the original node uses 15 dB transmission power level. We observed that the curve of Dm under the different transmission power level shifts to the right indicating larger Dm values. Thus, spoofing attacks launched by using different transmission power levels will be detected effectively in GADE. 802.15.4 network, the detection rate is above 90 percent when the distance between Pspoof and Porg is about 20 feet by setting the false positive to 5 percent. This is in line with the average localization estimation errors using RSS [8] which are about 15 feet. If the nodes are less than 15 feet away, they have a high likelihood of generating similar RSS readings, and thus the spoofing detection rate falls below 90%, but still greater than 70 %. However, when Pspoof moves closer to Porg, the attacker also increases the probability to expose itself.

**Table 1**
**HSRMA: Hit Rate, Precision, and F-Measure of Determining the Number of Attackers**

| *Number of Attackers* | *2* | *3* | *4* |
|---|---|---|---|
| 802.11Network,Hit Rate | 99.87% | 98.32% | 90.16% |
| 802.11Network,Precision | 98.88% | 91.52% | 99.76% |
| 802.11Network,F-measure | 99.31% | 95.65% | 95.32% |
| 802.11Network,Hit Rate | 99.95% | 96.14% | 88.82% |
| 802.11Network,Precision | 96.95% | 89.16% | 99.87% |
| 802.11Network,F-measure | 98.56% | 93.21% | 93.43% |

The detection rate goes to 100% when the spoofing node is about 45-50 feet away from the original node. So in these related operations were give a better performance But we proposed HSRMA has higher performance of its operations when compare to existing all methods. Normal node established the unique ID, Send location claim to all nodes, verify secret key, when the packets arrive to the node, the acts as relay to send packets to destination. Whereas attacker node extracts secret ID from the normal node, try to send packets to destination. The proposed work is analyzed by plotting the graph for SINR with fading and without fading for all nodes in the network as shown in Figure 4(a-b) and capacity of HSRMA is analyzed for different network nodes such as 2,3 and 4 and it found that the capacity has been increased for higher network nodes as shown in Figure 5(a-b).

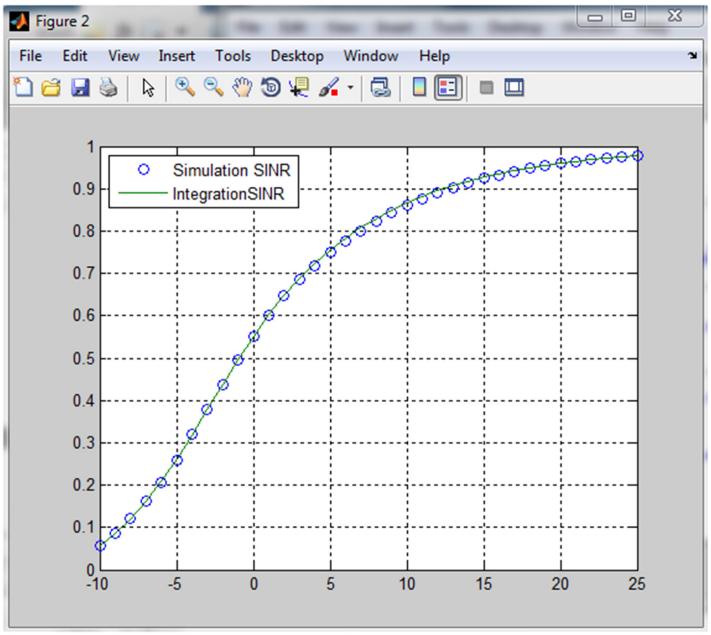


**Figure 4: (a) Performance level of SINR**

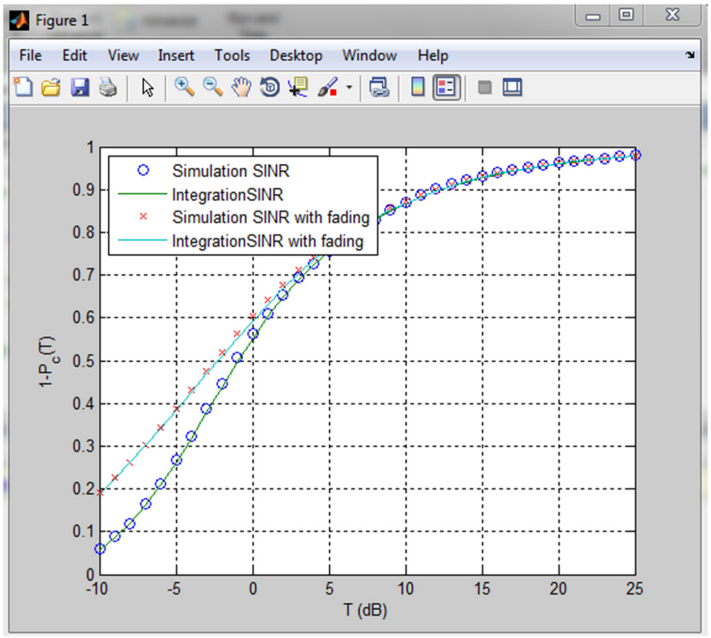


**Figure 4: (b) Performance level of SINR with fading**

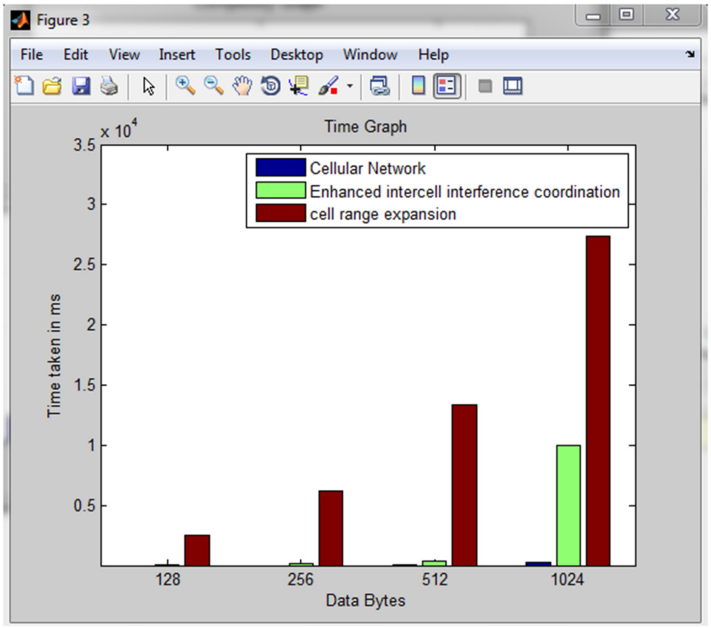


**Figure 5: (a) Performance graph between time data Bytes**

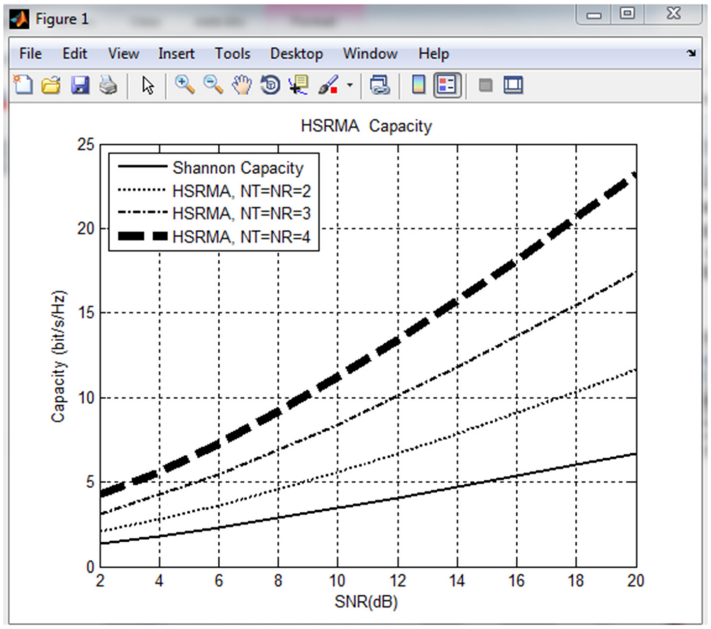


**Figure 5: (b) Performance level of HSRMA for different network size capacity**

## 4. CONCLUSION

In this proposed work, the designed protocol shows that HSRMA allows the management and creation of a network using spontaneous ad hoc wireless network for transmission of packet from source to destination. It will improves the services offered by users and information provided to other network using self-configuration that have unique IP address assigned to each and every node present in the network. The attacks detection rate is improved almost near to 100% as shown in Table 1 and the coverage area of the network improvised as compared with the previous existing network and observed that interferences between the packets and SINR are

optimized in the proposed technique. The channel capacity of HSRMA with different network sizes is increased as compared with the Shannon technique.

## REFERENCES


[1] Zengyou Sun and Chuanhui Hao, "Research on WLAN Networking Mode Based on Ad Hoc", 2nd International Symposium on Computer, Communication, Control and Automation (3CA 2013), 2013. The authors - Published by Atlantis Press.

[2] Samad Baseer, et.al, "A Review of Routing Protocols of Heterogeneous Networks", IJCA Special Issue on "Mobile Ad-hoc Networks", MANETs, 2010.

[3] Prabagarane Nagaradjane.et.al, "Performance of MUTP-aided MIMO systems over correlated frequency-selective wireless communication channels: a multi-cell perspective", EURASIP Journal on Wireless Communications and Networking 2012, 2012:194.

[4] Juan Wen, et.al, "On the Capacity of Downlink Multi-Hop Heterogeneous Cellular Networks ",IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, Vol. 13, No. 8, AUGUST 2014, pp 1536-1276.

[5] Rajkarn Singh,et.el, "A Multi-tier Cooperative Resource Partitioning Technique for Interference Mitigation in Heterogeneous Cellular Networks", The 2014 International Workshop on Resource Allocation, Cooperation and Competition in Wireless Networks, 978-3-901882-63-0/14/$31.00 ©2014 IEEE.

[6] Yujie Zhang, et.al, "Resource Allocation for Cognitive Radio-Enabled Femtocell Networks with Imperfect Spectrum Sensing and Channel Uncertainty", 0018-9545 (c) 2015 IEEE, DOI 10.1109/TVT.2015.2500902, IEEE Transactions on Vehicular Technology.

[7] A. Daeinabi,et.al, 'A Dynamic Almost Blank Subframe Scheme for Video Streaming Traffic Model in Heterogeneous Networks", 978-1-4799-7961-5/15/$31.00 ©2015 IEEE.

[8] Sihua Shao,et.al, "Design and Analysis of a Visible-Light Communication Enhanced WiFi System" Journal of Optical Communication Neywork, Vol. 7, No. 10, OCTOBER 2015.

[9] Bharat Shrestha, et.al, "An Analysis of Wireless Backhaul for Picocell Base Stations in Heterogeneous Networks", Globecom 2013 - Wireless Networking Symposium, 978-1-4799-1353-4/13/$31.00 ©2013 IEEE.

[10] Hsiang-Hung Liu.et.al, "Content-aware Spectrum and Power Allocation for Video Multicast in Two-tier Femtocell Networks", 978-1-4799-3083-8/14/$31.00 ©2014IEEE, IEEE WCNC'14 Track 4 (Services, Applications, and Business)

[11] Jia Yu. et.al, "Statistical Analysis of Capacity in Joint Processing Coordinated Multi-Point Systems", 978-1-4799-4146-9/14/$31.00 ©2014 IEEE, IEEE/CIC ICCC 2014 Symposium on Wireless Communications Systems

[12] Xi Chen.et.al, *User Partitioning Based Resource Allocation and Interference Coordination in Heterogeneous Networks*, 978-1-4799-4912-0/14/$31.00 ©2014 IEEE, 2014 IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications,

[13] Shuqi Qin.et.al, Quasi-distributed Uplink Interference Coordination in Co-channel HSPA+ Heterogeneous Network, 978-1-4577-1348-4/13/$31.00 ©2013 IEEE, 2013 IEEE 24th International Symposium on Personal, Indoor and Mobile Radio Communications: Mobile and Wireless Networks

[14] Yongyu Dai.et.al, "Adaptive Mode Switching Based on Statistical CSI for Downlink MIMO in Heterogeneous Network with RRH Deployment", 978-1-4673-6337-2/13/$31.00 ©2013 IEEE

[15] Thomas Wirth.et.al, "System-Level Performance of the MIMO-OFDM Downlink with Dense Small Cell Overlays", 978-1-4799-2390-8/13, 2013,IEEE

[16] Prabagarane Nagaradjane, et.el, "Performance of MUTP-aided MIMO systems over correlated frequency-selective wireless communication channels: a multi-cell perspective", EURASIP Journal on Wireless Communications and Networking 2012, 2012:194

[17] Mehdi Ait-Ighil.et.al, "Simplifying the propagation environment representation for LMS channel modelling", EURASIP Journal on Wireless Communications and Networking 2012, 2012:110

[18] Jianhua Zhang.et.al, "Analysis and modeling of spatial characteristics in urban microscenario of heterogeneous network", EURASIP Journal on Wireless Communications and Networking 2011, 2011:187

[19] Ghadir Madi.et.al, Impacts of impulsive noise from partial discharges on wireless systems performance:application to MIMO precoders, EURASIP Journal on Wireless Communications and Networking 2011, 2011:186

[20] Gulzaib Rafiq.et.al, "The impact of spatial correlation on the statistical properties of the capacity of nakagami-m channels with MRC and EGC", EURASIP Journal on Wireless Communications and Networking 2011, 2011:116.