A Novel Security Enhancement Strategy for Improving the Concert of CDMA Based Mobile Ad-Hoc Network

A. Swaminathan 1st
M.E (Comm. Engg. Student)
Dept of ECE, Annamalai University
Annamalai Nagar, Tamil Nadu, India
E-mail: rgaswami19@gmail.com

Dr. B. Santhana Krishnan 2nd
Assistant Professor
Dept of Electrical Engg., Annamalai University
Annamalai Nagar, Tamil Nadu, India
E-mail: ramyasugan@rediffmail.com

Dr. M. Ramaswamy 3rd
Professor
Dept of Electrical Engg., Annamalai University
Annamalai Nagar, Tamil Nadu, India
E-mail: aupowerstaff@gmail.com

Abstract: Mobile Ad-hoc networks have become an indispensable part of people’s daily life. Recent research has been shown that the physical layer security techniques become a more essential part in the wireless communications. As a result, security is an imperative and more challenging issue in wireless networks since the users might transmit their sensitive personal information (e.g., credit card details) over the wireless networks. The open communications environment makes wireless transmissions more vulnerable than wired communications to malicious attacks, including both eavesdropping and jamming for disrupting legitimate transmissions. Wireless air interface is open and accessible to both authorized and illegitimate users. This completely differs from a wired network, where communicating devices are physically connected through cables and a node without direct association is unable to access the network for illicit activities. Code division multiple access network is an example of multiple access, where several transmitters can send information simultaneously over a single communication channel with the optimum available bandwidth based on spread spectrum technology. It is proposed to develop an anti eavesdropping strategy for improving the performance of CDMA based network. Network Simulation has been conducted to evaluate the performance of proposed network. The results are obtained in terms of the performance indices with the aid of Zero knowledge protocol to identify the type of attackers and the data are routed through AODV routing pattern. The new approach shows that the proposed outcome is an extended enhancement of network security.

Keywords: Transmission Scheduling; Eavesdropping; Zero Knowledge Algorithm; Secrecy Outage Probability; Secrecy Rate; Rayleigh Fading.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have attracted much recent research interests and have been widely studied due to many military as well as civilian applications [1]. A typical wireless sensor network normally consists of some small, inexpensive, and low-power sensors, which are deployed over a region and may communicate with a remote processor over wireless links. WSN nodes can be categorized as source node, sink node and intermediate nodes depending upon functionality in environment [2]. Sensor technology is marked as one of the world’s emerging technology by recent technological review. The deployment of WSNs, which usually consist of plenty of small autonomous devices called sensor nodes, has been accelerated by the progression in sensor network technology. Due to cost effectiveness, the wireless sensor networks are quickly gaining enormous popularity for solving world challenges. Sensor nodes in WSNs are inherently resource-constrained. The main issue in the wireless sensor network is the energy of the sensor nodes and battery-operated nodes have limited processing capability and very low storage capacity [3]. These limitations are due to limited energy and physical size of the sensor nodes.

A typical WSN is composed of multiple sensor nodes that periodically send updates to an in-situ base station (BS). In such a network, the BS becomes a natural focal point for the adversary since the unique role of the BS would likely allow the most impactful attack possible against the target WSN to be launched with the least amount of effort. Sensor nodes are unattended and even deployed in the hostile environments, which demand careful security consideration in the design of WSN. Because of those constraints, the conventional security mechanisms with high computation complexity are not feasible for WSNs.

Code division Multiple Access (CDMA) is an example of multiple access, where several transmitters can send information simultaneously over a single communication channel [4]. It allows several users to share a band of frequencies without undue interference between the users. CDMA employs spread spectrum technology with a special coding scheme. Most modulation schemes try to minimize the bandwidth utilization since it is a limited resource [5]. However, spread spectrum techniques use a transmission bandwidth that is several orders of magnitude greater than the minimum required signal bandwidth. The reasons for doing this were military applications including guidance and communication systems. These systems were designed using spread spectrum because of its security and resistance to jamming [6]. Asynchronous CDMA has some level of privacy built in because the signal is spread using a pseudorandom code, this code makes the spread spectrum signals appear to random properties.

Mobile ad-hoc networks are vulnerable to security attacks due to the broadcasting transmission mediums. Furthermore, wireless networks have probably collected through direct site surveillance. Relatively, ad-hoc networks strengthen the privacy problem because they make large volumes of data easily available through remote network access [7]. Hence, attackers need not be physically present to maintain long time. They can gather information at low-risk in unknown manner. Security is a critical concern in mobile ad-hoc networks due to the open wireless medium. Physical layer security, which exploits the physical characteristics of wireless channels for secure transmission, has attracted much attention recently [8]. The maximum achievable secrecy rate is referred to as secrecy capacity which shows that as long as the eavesdropper’s channel is a degraded version of the receiver’s channel, perfect secrecy can be achieved without any key. Any receiver within the range of a wireless transmission can potentially overhear the transmitted information.

II. Related Work

A new compressive sensing based encryption scheme has been proposed for wireless sensor network [9]. It has been found that proposed algorithm reduces the data error without additional computation cost even in both normal and attack condition. Investigation of distortion outage minimization problem in presences of eavesdropper has been proposed for wireless sensor network [10]. It has been found that the proposed scheme provides better performance achieved by adding multiple receive antennas at the fusion center. A multiple phantom with multiple fake source schemes has proposed for wireless sensor network [11]. It has found that proposed algorithm is efficient to hide the location source node thereby increasing network life time.

A tractable frame work has been suggested for three tier WSN using stochastic geometry [12]. It has been found that the proposed method provided security enhancement with multiple antenna at the access point. Two anti-eavesdropping schemes have been proposed for interference alignment based network [13]. It has been found that the proposed model gives better performance improvement through various security techniques. A novel network key management schemes has been proposed for WSN [14].It has been found that the proposed schemes gives over all analysis based on loaded key utilization, resources consumption and rigidity against node captured. A distributed anonymity boosting techniques has been suggested for WSN [15]. It has been found that the proposed method increased its anonymity on-demand based on real time measurement there by conserve the resources and simulation result shows the effectiveness of proposed schemes [16].

This paper tries to provide an insight into the various aspects and implementation of security practices in CDMA based network and Security against eavesdropping can be achieved by using zero knowledge protocol.

III. Problem Statement

The ad-hoc network is designed with N nodes and each node has number of data to transmit to their corresponding destination. Besides, the nodes are allowed to trade the data through wireless way to any other node in the network. The aim is to build up an anti eavesdrop strategy with aid of zero knowledge protocol with view to increase the performance of the CDMA based network. The network simulator-2 (NS2) based simulation results highlight the suitability of proposed strategy to ensure the security enhancement of the network..

IV. Proposed Algorithm

The objective of this proposed method is to develop mechanism that protects the closed MANET against malicious behavior from outside nodes as well as inside nodes by Zero Knowledge Protocol (ZKP) authentication method. Authentication system in wireless ad hoc network can use ZKP algorithms because it has the unique characteristic and properties like Completeness, soundness and zero knowledge. A ZKP is a special cryptographic algorithm is used to verify the identification based on complex mathematical analysis which requires heavy computations time. The purpose of ZKP protocols is to help a prover convince a verifier that he or she holds some knowledge (usually secret), without leaking any information about the knowledge during the verification process (zero knowledge). If the declaration is true, no fraud verifier absorbs anything other than this circumstance. It was unveiled by presenting that every fraud verifier has some simulator that, assumed only the declaration to be proven (and no entree to the prover), can generate a transcript that “looks like” and contact between the honest prover and the fraud verifier.

It must be noted that the concept of proof in ZKP is different from the traditional mathematical concept.

Mathematical proofs are strict, using either self evident statements or statements obtained from proofs established beforehand. ZKP proofs are more similar to the dynamic process used by humans to establish the truth of a statement throughout the exchange of information. Furthermore, instead of presenting a static proof for a statement, the prover involves the verifier in a process in which he tries to convince the verifier of the truth of the statement interactively.

Some promising security attacks associated with authentication are Man-In-The-Middle attack (MITM), Denial of Service (DoS) attack, Eaves dropping and Replay attack. MITM also known as a bucket brigade attack in cryptography and computer security is a form of active eavesdropping in which the attacker watches on the link between the verifier and the prover and intercepts all authentication messages going between the two parties. The attacker impersonates the sender with respect to receiver and vice versa without the knowledge of either parties that they have been attacked.

The main goal of DoS attacker is to prevent legitimate users from using system services, and to have impact on an availability of the system. The malicious node does perform a DoS attack by flooding irrelevant data to consume most of the resources of a particular node or entire network such as power, storage capacity or computational resource.

Eavesdropping is a passive attack in which a node simply observes sensitive information. This information which is overheard by a malicious node can be used later to ruin the security in the network. Sensitive information such as location, public key, private key or password can be fetched by the eavesdropper.

Replay attack is a form of network attack in which the valid data is repeatedly transmitted across the network to inject the network routing traffic by a fraudulent node or attacker. These attacks can be made void if the system has an efficient authentication method, bearing in mind the characteristics of MANET while designing.

Flow Chart

The following flow diagram seen in figure 1 explains the function of proposed approach.

Pmin	Minimum power
Pmax	Maximum power
X_j	Transmitter signal
Y_j	Received signal
Rs	Secrecy rate
C_{jj}	Shannon channel capacity
β	Signal to noise ratio
ρ	Fading variance
N_o	Variance
h_{jj}	Represents a fading coefficient of the legitimate channel
h_{je}	Represents a fading coefficient of the wiretap channel

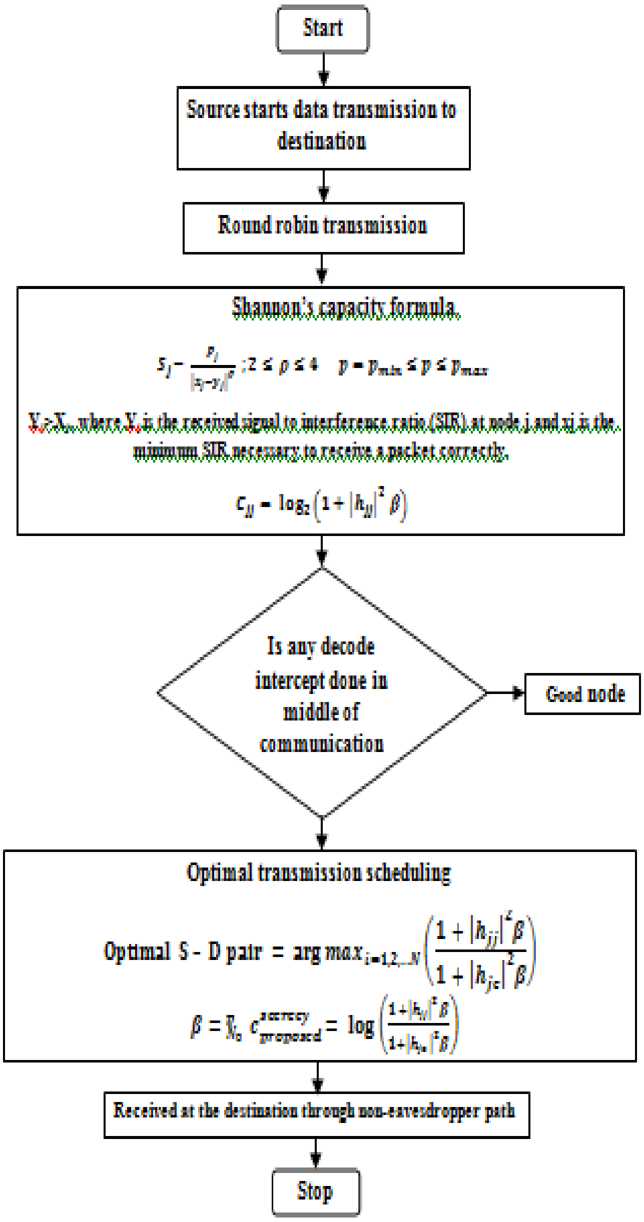

Start
Source starts data transmission to destination
Round robin transmission
Shannon's capacity formula.
$S_j = \frac{P_j}{|x_j - y_j|^{\rho}}$;2 ≤ ρ ≤ 4 $p = p_{min} \le p \le p_{max}$
Y_j>X_j, where Y_j is the received signal to interference ratio (SIR) at node j and xj is the minimum SIR necessary to receive a packet correctly.
$C_{jj} = \log_2\left(1 + |h_{jj}|^2 \beta\right)$
Is any decode intercept done in middle of communication
Good node
Optimal transmission scheduling
Optimal S - D pair = $\arg max_{i=1,2,\dots N}\left(\frac{1+|h_{jj}|^2\beta}{1+|h_{je}|^2\beta}\right)$
$\beta = \aleph_0$ $C^{secrecy}_{proposed} = \log\left(\frac{1+|h_{jj}|^2\beta}{1+|h_{je}|^2\beta}\right)$
Received at the destination through non-eavesdropper path
Stop

Figure 1 Flow Diagram of Proposed Scheme

V. Simulation Results

The proposed scheme exploring the performance of the secured communication of a mobile ad-hoc network designed with two hundred mobile nodes spread in an area of 1000 m X 1000 m as illustrated in Figure 2 and Figure 3 shows the anti eavesdropping network. It involves the method of exchanging the data of size 1000 KB from three sources to corresponding destination nodes. The performance indices like Packets Received, Packet Loss, Throughput, Energy consumption, Packet Delivery Ratio (PDR) and Routing Delay are calculated through NS2simulation.

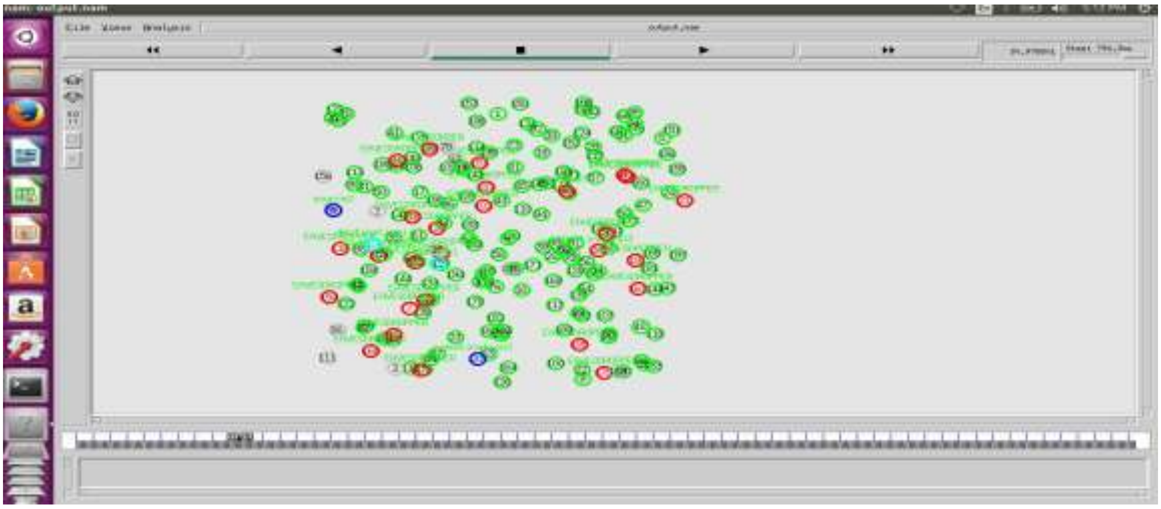


Figure 2 Simulation Model

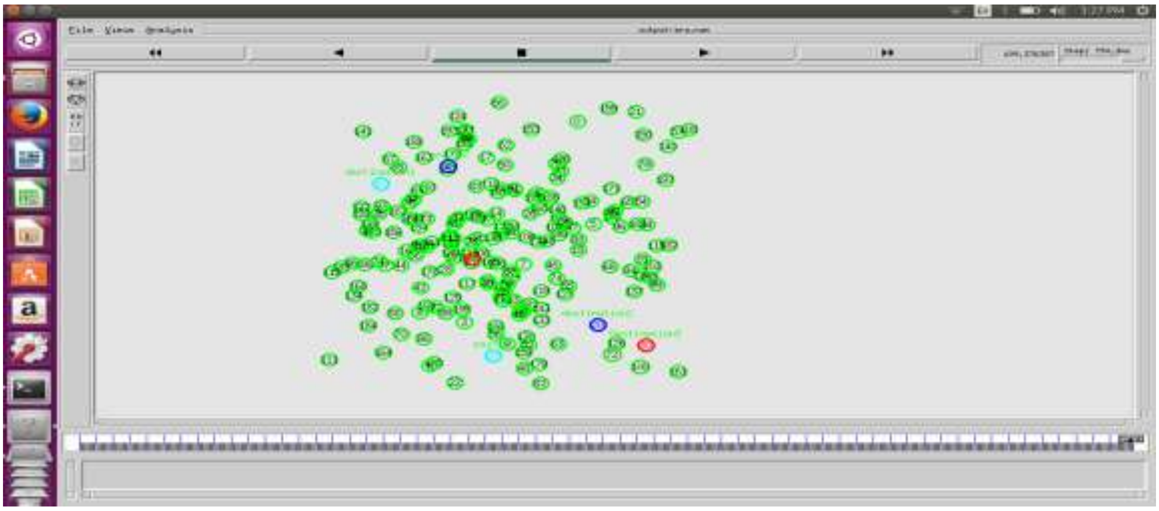


Figure 3 Attackers Free Network Model

It is seen from Figure 4 that the proposed algorithm consumes minimum energy when compared with network having 25 attackers and offers the minimal routing overhead thereby increasing the life time of the network.

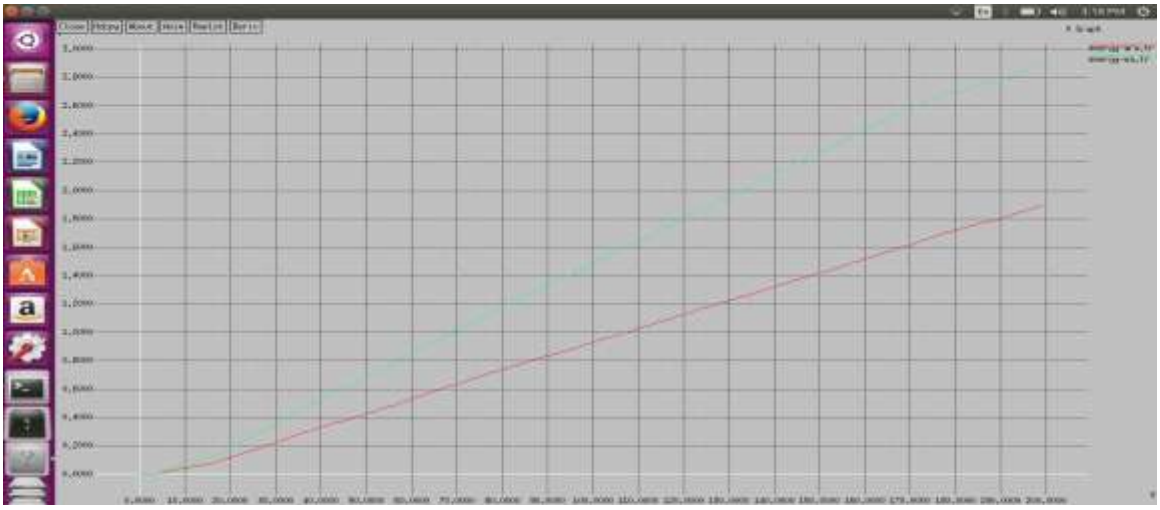


Figure 4 Energy Consumed vs Time

The proposed method as outlined in Figure 5 is suitable for maximum number of packets received from identified source to destination with secured data transfer. The minimum delay as seen through Figure 6 related to proposed scheme explores the suitability of the overall network security along with performance improvement when compared with attacker network.

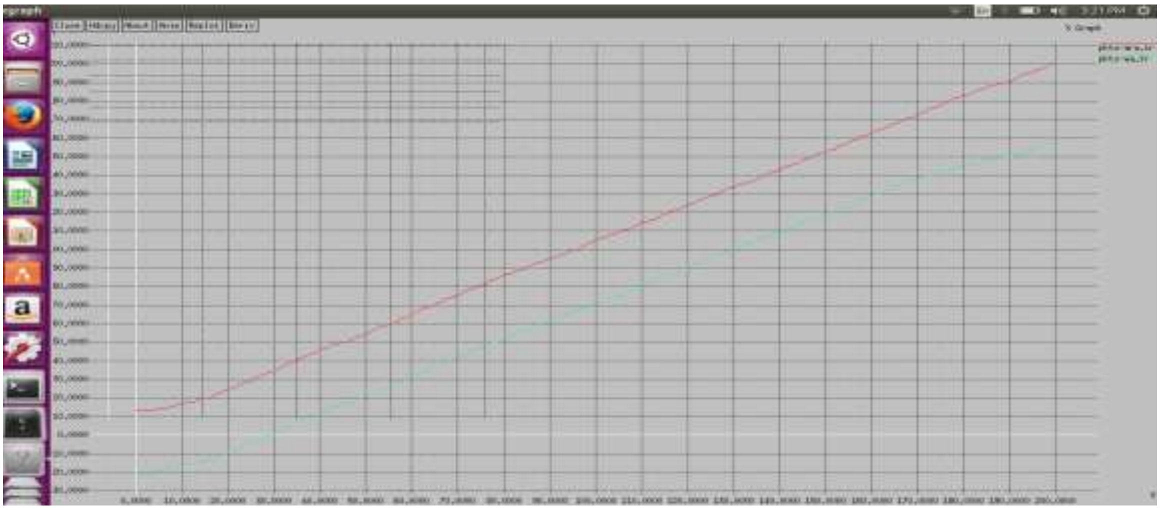


Figure 5 Packets Received vs Time

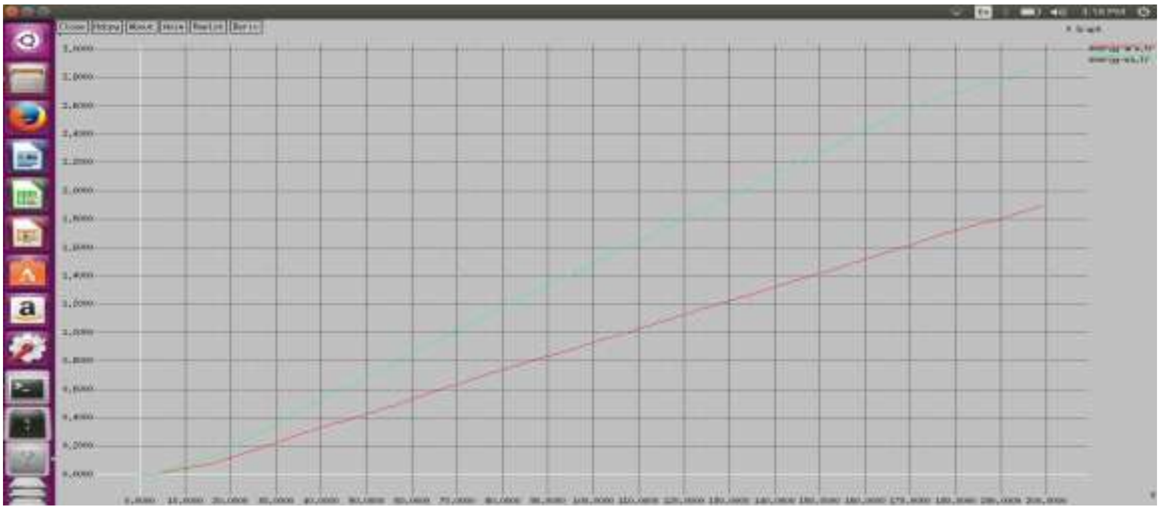


Figure 6 Routing Delay vs Time

The Packet Delivery Ratio (PDR) of the network under study is seen from Fig.7. It follows that the proposed routing pattern endow with a greater value rate with its counterpart.

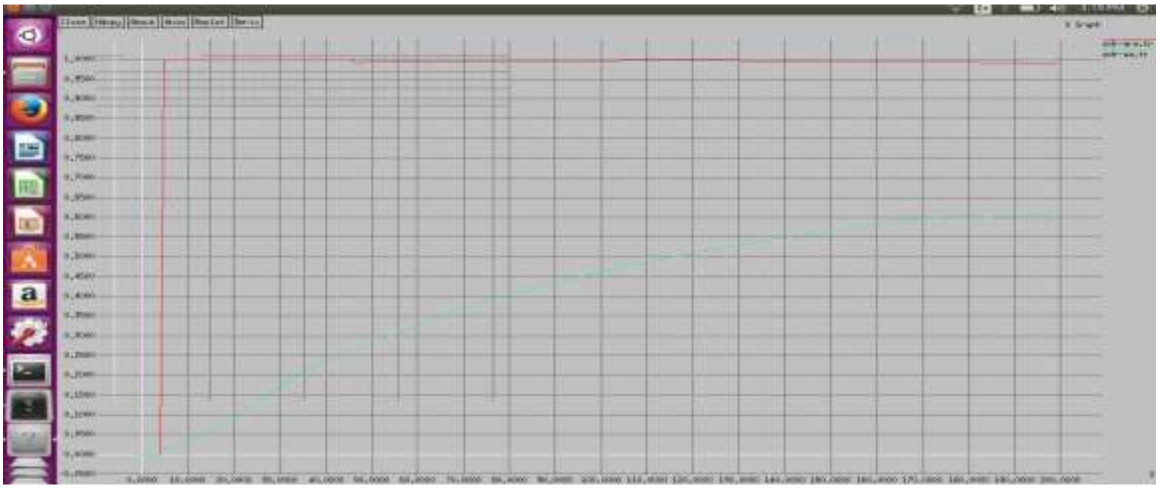


Figure 7 PDR vs Time

The proposed method provides minimum loss of packets as compared to their counterpart as seen in Figure 8 and gives an enhancement of the network security and efficiency. It is observed from Figure 9 that the proposed scheme gives an incredible throughput for the same size of the data secured packets transmitted when compared with its matching part.

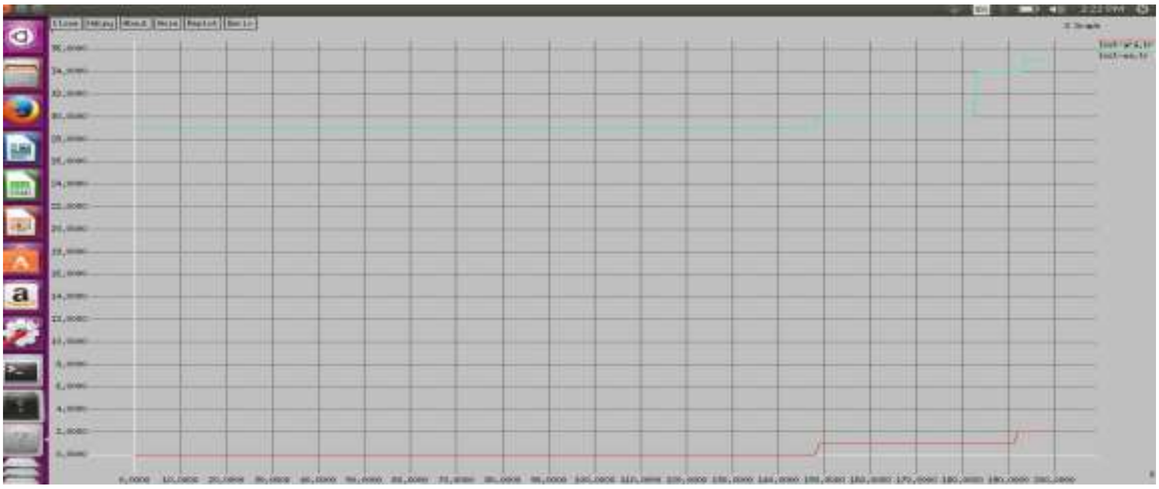


Figure 8 Packet Loss vs Time

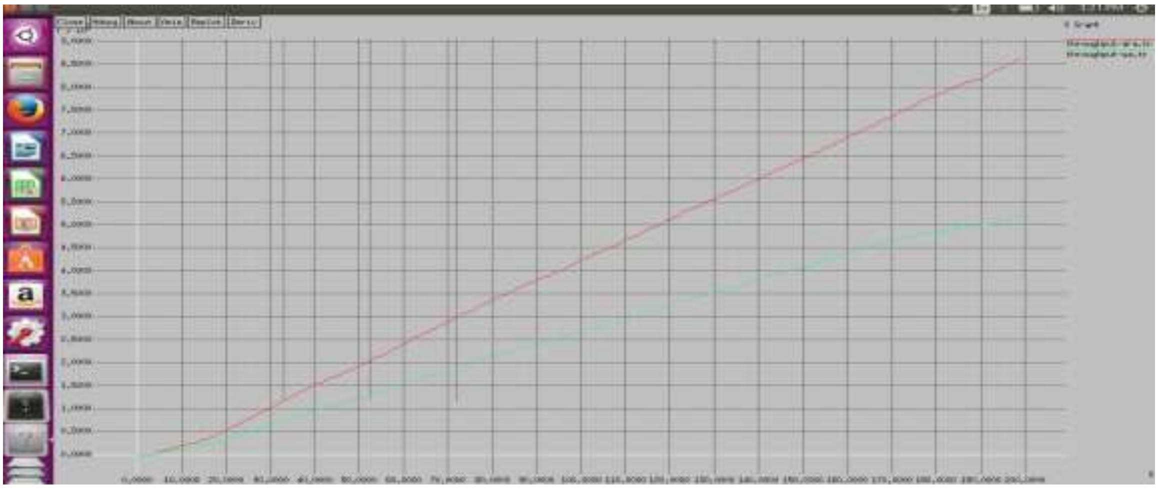
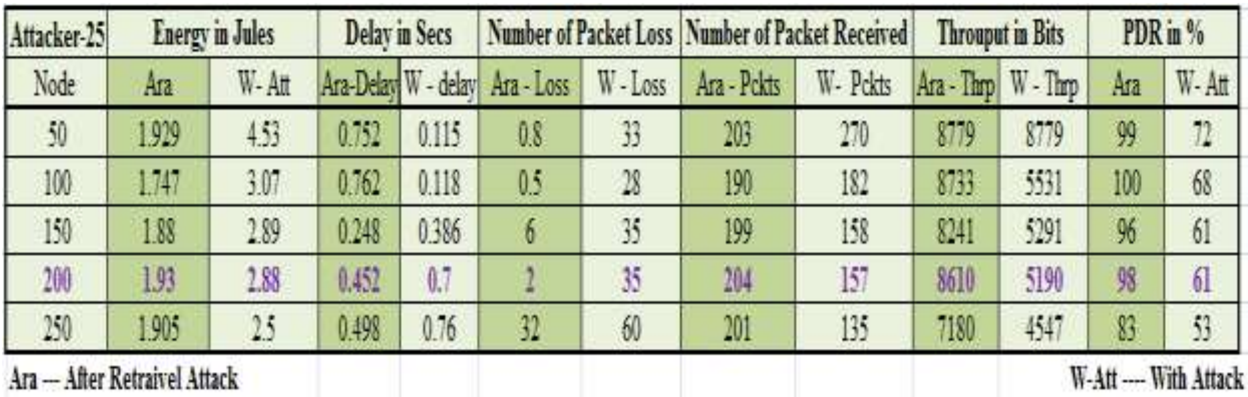


Figure 9 Throughput vs Time

The performance metrics listed in Table 1 are derived for cdma based anti eavesdropping communication strategy with data size of 1000 KB. The network is allowed to vary the number of nodes from 50 to 250 with secured data transmission based on round robin scheduling. The investigation proves that the algorithm is stable in its assignment and helps to validate the rewards of the proposed method.

Table 1 Performance Comparison with Node Variation



Attacker-25	Energy in Jules		Delay in Secs		Number of Packet Loss		Number of Packet Received		Throuput in Bits		PDR in %	
Node	Ara	W- Att	Ara-Delay	W - delay	Ara - Loss	W - Loss	Ara - Pckts	W- Pckts	Ara - Thrp	W - Thrp	Ara	W- Att
50	1.929	4.53	0.752	0.115	0.8	33	203	270	8779	8779	99	72
100	1.747	3.07	0.762	0.118	0.5	28	190	182	8733	5531	100	68
150	1.88	2.89	0.248	0.386	6	35	199	158	8241	5291	96	61
200	1.93	2.88	0.452	0.7	2	35	204	157	8610	5190	98	61
250	1.905	2.5	0.498	0.76	32	60	201	135	7180	4547	83	53

Ara -- After Retraivel Attack W-Att --- With Attack

VI. Conclusion

A new anti eavesdrop transmission strategy for cdma based mobile ad-hoc network has been developed to adapt secure data transfer in energy constraint network. The performance metrics of the scheme has been measured through various attacks in the network. The ns2 simulation results are compared with attack free network to elucidate its security enhancement. The idea of the proposed scheme has been taken in terms of higher throughput, PDR and number of packets received in association with attack free strategy. Moreover the proposed method has been coined to extract an improved security enhancement over conventional secured CDMA network and expose the fitness of the new algorithm for present day applications. The graphs have been revealed to highlight the effectiveness in terms of least delay, packet loss and energy consumption. The results have been association with higher echelons of secured data transfer that considerably improves the life time of the CDMA based network.

Acknowledgment

The authors thank the authorities of Annamalai University for providing the necessary facilities in order to accomplish this piece of work.

References

[1] Francisco José Estévez , Peter Glösekötter and Jesús González "DARAL: A Dynamic and Adaptive Routing Algorithm for Wireless Sensor Networks", Sensors, pp. 1-22, 2016.

[2] Mansour Abdulaziz and Robert Simon, "Multi-Channel Network Coding in Tree-Based Wireless Sensor Networks", IEEE International Conference on Computing, Networking and Communications, Wireless Ad Hoc and Sensor Networks Symposium, pp. 924-930, 2016.

[3] Ji Wu, Qilian Liang, Baoju Zhang, and Xiaorong Wu , “Security Analysis of Distributed Compressive Sensing-Based Wireless Sensor Networks”, The Proceedings of the Second International Conference on Communications, Signal Processing and Systems, Springer International Publishing, pp. 41-49, 2014.

[4] Nitish Aggarwal , Rachit Gupta and Pallavi Saxena ,” Comparative Study of TDMA and CDMA Technology”, International Journal for Research in Applied Science & Engineering Technology, Volume 2 Issue XI, pp.100-102, 2014.

[5] Tawfig Eltaif, Hesham A. Bakarman, N. Alsowaidi, M. R. Mokhtar, Malek Harbawi, “Reduction of Multiple User Interference for Optical CDMA Systems Using Successive Interference Cancellation Scheme”, World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering Vol:9, No:7, pp.697-673, 2015.

[6] Jinho Choi and Euiseok Hwang, “Secure Multiple Access based on Multicarrier CDMA with Induced Random Flipping”, IEEE Transactions on Vehicular Technology, pp.1-10, 2016.

[7] Waheb A. Jabbar, Mahamod Ismail, and Rosdiadee Nordin, ”On the Performance of the Current MANET Routing Protocols for VoIP, HTTP, and FTP Applications”, Journal of Computer Networks and Communications Volume,PP.1-12, 2014.

[8] Rajeshwar Sharma, Tarun Sharma and Aditi Kalia, “A Comparative Review on Routing Protocols in MANET ” , International Journal of Computer Applications Volume 133 – no.1, pp. 33-38, 2016.

[9] Devdatt Nadre and Balaso N. Jagdale, “Security for source node privacy in wireless sensor network”, International journal of advanced research in computer science and software engineering, Volume 5, Issue 2, pp.752-757 , 2015.

[10] Wu, J., Liang, Q., Zhang, B.,and Wu, X., “Security analysis of distributed compressive sensing-based wireless sensor networks”, In *Proceedings of the Second International Conference on Communications, Signal Processing, and Systems, CSPS 2013,* Volume. 246, pp. 41-49, 2013.

[11] x guo, as leong and s dey “ power allocation for estimation outage minimization with secrecy outage constraints” Australian communications, volume 6, pp.71-76, 2016.

[12] Pradeep kumar roy, rimjhim, jyoti prakash singh and prabhat kumar “An efficient privacy preserving protocol for source location privacy in wireless sensor networks”, wireless communications, signal processing and networking (wispnet) international conference, volume.177, pp.1093-1097, 2016.

[13] Yansha Deng, Lifeng Wang, Maged Elkashlan, Arumugam Nallanathan and Ranjan K. Mallik “Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach” IEEE Transactions on Information Forensics and Security Volume.11, Issue: 6, pp.1-11, 2016

[14] Nan zhao, f. Richard yu, Ming li and victor c. m. leung “Anti-Eavesdropping Schemes For Interference Alignment (IA)Based Wireless Networks” ieee transactions on wireless communications , volume: 15, issue: 8, pp.1-15, 2016

[15] Jon R. Ward and Mohamed Younis “Base station anonymity distributed self assessment In Wireless Sensor Networks” Intelligence and Security Informatics (ISI), 2015 IEEE International Conference, volume. 277, pp.103-109, 2015.

[16] Nazmul Islam and M. A. Moyeen “An Empirical Study on Key Management Schemes of Wireless Sensor Network” International Journal of Computer Applications, volume.77, pp.30-34, 2016

AUTHOR’S BIOGRAPHIES

Swaminathan. A obtained his Bachelor’s degree in Electronics and Communication Engineering from Panimalar Engineering College under Anna University, Chennai, in 2015. He is on the way to obtaining his Master’s degree in Communication Engineering. His areas of interest include Wireless Sensor and Mobile Ad-Hoc Networks.

Santhana Krishnan. B obtained his Bachelor’s degree in Electrical and Electronics Engineering from SRM Engineering College under Madras University in 1999 and his Master’s degree in Power Systems Engineering from Annamalai University in 2005. He is currently working as an Assistant Professor in the Department Of Electrical Engineering at Annamalai University. He obtained his Doctoral Degree in Electrical Engineering from Annamalai University in 2016. He has a number of publications in International Journals to his credit. His areas of interest include Personal Computer Systems, Communication Engineering, Computer Communication, Wireless Sensor Networks, Power System Voltage Stability Studies and Intelligent Control Strategies.

Ramaswamy. M obtained his Bachelor’s degree in Electrical and Electronics Engineering from Madurai Kamaraj University in 1985, Master’s Degree in Power Systems Engineering in 1990 and Doctoral degree in Electrical Engineering in 2007 from Annamalai University. He is currently serving as a Professor in the Department of Electrical Engineering at Annamalai University. He has a number of publications in National and International journals to his credit. His areas of interest include Power Electronics, Solid State Drives, Power System Voltage Stability Studies, HVDC transmission, Fuzzy control techniques and Communication Networks.