

Game Theoretical Approach For Anonymous Secure Routing In Manets

K.Swapna¹, Sanjay Kumar Suman² and L. Bhakyalakshmi³

¹*Course of Embedded System Technologies, Velammal Institute of Technology,
Panchetti-601204, TN, India*

²*Associate professor, Dept of ECE, Velammal Institute of Technology, Panchetti-
601204, TN, India*

¹*kumarswapna01@gmail.com, ²velammal.ecetimes@gmail.com*

Abstract

In the adversarial environments, anonymous routing is unavoidable for communication hence, node unidentifiability plays a key role in Manets. Security is inappropriate in such environments. In this paper, game theoretical approach and AASR (Authenticated Anonymous Secure Routing) protocol is used to tackle the problems concerned with security issues without establishing the node identity. Though existing systems preserve the node identities using pseudonyms, they lack in preventing attackers to interfere in the middle of communication. Proposed system aims at resolving this problem. Game theory has been implemented in making strategic decisions by the nodes during network communication. The mechanism of group signature is utilized here for each route message, which ensures high security. Using onion routing, the security is provided without unveiling the node identity as each node information is encrypted during the transfer of packets. Simulation is performed using ns2, which provides better results than the existing protocols for providing security.

Keywords: Game theory ,Authenticated Anonymous Secure Routing (AASR), Node unidentifiability, Manets

Introduction

Wireless networks provide unprecedented freedom and mobility for a growing number of laptop and PDA users who no longer need wires to stay connected with their workplace and the Internet. Wireless networks are divided into two categories. Infrastructure wireless network and infrastructure less or ad hoc wireless network.

Infrastructure network have fixed network topology. It has a fixed point called base station or access point through which the wireless nodes communicate. But the significant element, the base station might be connected through a wired link. All of

the wireless connections must pass from the base station. In case of multiple base stations the communication depends on certain criteria.

Ad hoc networks are infrastructure less networks that are complex distributed systems. Each node in the adhoc network can also act as a router. Adhoc networks have a permanent infrastructure and the nodes can either enter or leave the network at anytime. They can be stationary or mobile. Based on this, adhoc networks can be divided into two types. one is static ad hoc networks (SANET) and the other one is called mobile ad hoc networks (MANET). Adhoc networks can be deployed quickly and are very flexible. Thus it is suitable for the emergency situation. But on the other side it is also very difficult to handle the operation of ad hoc networks, as there will be dynamic topology change and each node acts independently. To solve this various routing protocols are introduced. The two main categories of routing protocols are table driven routing protocol and on-demand routing protocol. The protocols to be used in the MANET should have the following features.

- The protocol should adapt quickly to topology changes and should provide loop free routing.
- The protocol should provide multiple routes from the source to destination; this will solve the problems of congestion to some extent and supports reliability in case of link or node failure.
- The protocol should have minimum control message overhead due to exchange of routing information when topology changes occur.
- The protocol should use minimum resources like bandwidth, power and should support Quality of Service (QoS) and security.

As the explosive growth of the Internet and rapid adoption of wireless technology continues, it is clear that there will be an increasing demand for wireless data services. The combination of voice, multimedia, data traffic, file transfer and other real time traffic tends to increase interference. To transfer real-time and non real-time applications in interference prone and dynamic natured wireless medium requires a layered architectural model which adapts dynamic changes in the environments by exchanging critical information.

Related Work

The two main methods to provide security to a system are prevention based approaches and detection based approaches. Earlier models dealt with these models individually. Here both these approaches are considered together. But in case of networks with centralized coordination there is a lack in perfect security, as fault in single node can lead to the damage of the entire network [1].QoS can be improved by cooperative communication in mobile adhoc Network (MANETs).Idea behind is single-antenna mobile nodes in a Multi user Scenario can share their antennas in a manner that creates a virtual multiple- input and multiple-output (MIMO) system. Single antennas with multi radio networks are traditionally create more traffic in the network[2].In mobile ad hoc networks, nodes have the inherent ability to move aside from conducting attacks to maximize their utility and cooperating with regular nodes to deceive them, malicious nodes get better payoffs with the ability to move. Regular

nodes consistently update their beliefs based on the opponents' behavior, while malicious nodes evaluate their risk of being caught to decide when to flee. Some possible countermeasures for regular nodes that can impact malicious nodes' decisions are presented as well. Here we can observe only the single hop neighbors, it is not suitable for overall network [3]. Continuous user authentication is an important prevention-based approach to protect high security mobile adhoc networks (MANETs). On the other hand, intrusion detection systems (IDSs) are also important in MANETs to effectively identify malicious activities. The policies derived from structural results are easy to implement in practical MANETs but we are using centralized nodes [4]. As networks become ubiquitous in people's lives, users depend on networks a lot for sufficient communication and convenient information access. Game theoretic approaches have been introduced as a useful tool to handle those tricky network attacks. Two categories, attack-defense analysis and security measurement are dealt in two models cooperative game models and non-cooperative game models with the latter category consisting of subcategories but there is no algorithm for energy efficiency routing [5]. To alleviate the problem of unwanted interference and power issues due to centralized network pricing scheme is introduced. maintains control packets and data packets in separate queues in FIFO order. Currently, this scheme is used in most comparison studies about mobile ad hoc networks [6]. Various techniques are followed for detecting intruders and safeguarding the information. This provides clear decision and control framework mechanisms [7]. In case of unauthorized and distributed system, where there is no centralized coordination, a game theoretic approach is implemented considering the attacker and the individual node as two different players [8]. Though data distribution is the important goal, the individual nodes focus in increasing their battery life-time and power preservation. The suggested document is designed at accomplishing these goals without limiting on the data distribution. Here equity points are formulated in obtaining route which act as a balance between preserving power and completing data distribution. In this document the writer has suggested two different MAC strategies 1) distributed strategy for adhoc systems 2) coordinated systems for infrastructure systems [9]. Ossama Younis, Marwan Krunz and Fan Wang presented an idea to enhance the spatial reuse and energy consumption of mobile adhoc networks (MANET). The previously defined algorithm expected additional equipment expenses and also did not fully utilize the potential of the power which are overcome by the Transmission Power Control (TPC). The authors have proposed a new algorithm called game theoretic power control MAC protocol (GMAC). The main goal of this algorithm is to improve the throughput and energy consumption. This also allows multiple efficient users with respect to Nash equilibrium (NE) [10]. In order to reduce the interference of each node and to consume battery lifetime of each node, a novel method is proposed to achieve maximal power level [11]. Appropriate data rate and power are chosen by the users while providing high throughput and reduced resource utilization [17]. C.K. Tan, M.L. Sim and T.C. Chuah tried to incorporate non cooperative game theory in the field of adhoc networks where there is a lack of centralized coordination. Here co-channel interference is minimized especially in the infrastructureless adhoc networks. The two main parameters that are combined here

wormhole link is established, the adversary captures wireless transmissions on one end, sends them through the wormhole link and replays them at the other end.

The severity of the wormhole attack comes from the fact that it is difficult to detect, and is effective even in a network where confidentiality, integrity, authentication, and non-repudiation (via encryption, digesting, and digital signature) are preserved which is shown in Fig 2.

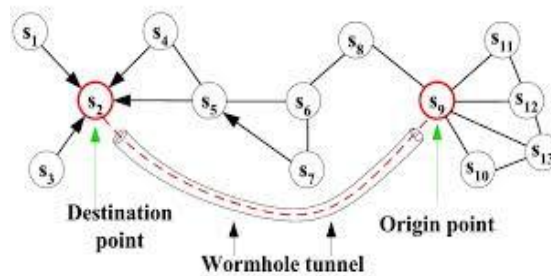


Figure 2: Wormhole Attack

3) Flooding attack:

The main aim of the flooding attack is to exhaust the resources of the network such as battery power etc. Furthermore an attacker can influence the network performance, by hindering the proper execution of routing algorithm (in routing discovery phase). By RREQ flooding, it is possible for an attacker to send multiple RREQs to non-existing recipient in a very short period of time, using the AODV protocol of MANET. The avalanche of RREQs all over the network leads to consumption of the battery power and the network bandwidth, causing DoS as in Fig 3.

As a countermeasure against the flooding attack every network participant (actual authentic user or simply node) can compute and monitor the evaluation of all neighbors RREQ, and in case of outmatching of the RREQs' limit, which is preliminarily defined, the specific neighbor node comes with its ID in a blacklist. By this way the authentic/actual node knows, that it should not receive any RREQs from its neighbors, recorded in its blacklist. Furthermore the efficiency of this countermeasure can be enhanced if the RREQ limit is not preliminarily defined (fixed), but is computed on hand of statistical analysis over RREQ, so the risk of attack with varying flooding rates to be minimized.

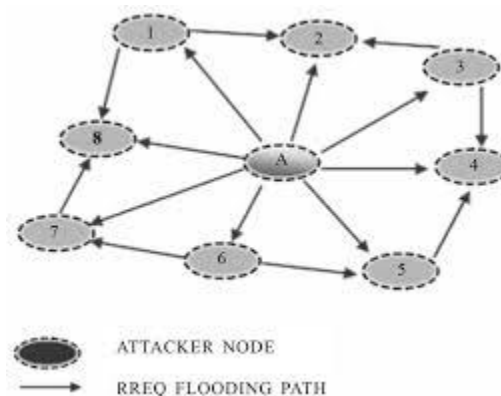


Figure 3: Flooding Attack

B. Network Security Tools

1. Antivirus software packages:

These packages counter most virus threats if regularly updated and correctly maintained.

2. Secure network infrastructure:

Switches and routers have hardware and software features that support secure connectivity, perimeter security, intrusion protection, identity services, and security management.

Dedicated network security hardware and software-Tools such as firewalls and intrusion detection systems provide protection for all areas of the network and enable secure connections.

3. Virtual private networks:

These networks provide access control and data encryption between two different computers on a network. This allows remote workers to connect to the network without the risk of a hacker or thief intercepting data.

4. Identity services:

These services help to identify users and control their activities and transactions on the network. Services include passwords, digital certificates, and digital authentication keys.

5. Encryption:

Encryption ensures that messages cannot be intercepted or read by anyone other than the authorized recipient.

People use encryption to change readable text, called plaintext, into an unreadable secret format, called cipher text. Encrypting data provides additional benefits besides protecting the confidentiality of a message. These advantages include ensuring that

messages have not been altered during transit and verifying the identity of the sender. All of these benefits can be realized by using any of these encryption methods.

There are three basic encryption methods:

- Hashing
- Symmetric cryptography
- Asymmetric cryptography

These three forms depend on cryptography, or the science of scrambling data.

i. Hashing Encryption:

Hashing creates a unique, fixed-length signature for a message or data set. Hashes are created with an algorithm, or hash function, and are used for comparing sets of data. Since a hash is unique to a specific message, even minor changes to that message result in a dramatically different hash, thereby alerting a user to potential tampering.

A key difference between hashing and the other two encryption methods is that once the data is encrypted, the process cannot be reversed or deciphered. Some common hashing algorithms are Message Digest 5 (MD5) and Secure Hashing Algorithm (SHA).

ii. Symmetric Methods:

Symmetric cryptography is one of the oldest and most secure encryption methods. It is also called private key cryptography as the key used for encrypting and decrypting the code should be very secure. A sender encodes a message into cipher text using a key, and the receiver uses the same key to decode it.

People can use this encryption method as either a "stream" cipher or a "block" cipher, depending on the amount of data being encrypted or decrypted at a time. A stream cipher encrypts data one character at a time as it is sent or received, while a block cipher processes fixed chunks of data. Common symmetric encryption algorithms include Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA).

iii. Asymmetric Forms:

Asymmetric or public key cryptography is, potentially, more secure than symmetric methods of encryption. This type of cryptography uses two keys, a "private" key and a "public key," to perform encryption and decryption. The use of two keys overcomes a major weakness in symmetric key cryptography, since a single key does not need to be securely managed among multiple users.

In asymmetric cryptography, a public key is freely available to everyone and used to encrypt messages before sending them. A different, private key remains with the receiver of cipher text messages, who uses it to decrypt them. Algorithms that use public key encryption methods include RSA and Diffie-Hellman.

RSA (algorithm)

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman.

A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key.

Security management:

None of these approaches alone will be sufficient to protect a network, but when they are layered together, they can be highly effective in keeping a network safe from attacks and other threats to security. In addition, well-thought-out corporate policies are critical to determine and control access to various parts of the network.

SHA (algorithm)

The four SHA algorithms are structured differently and are distinguished as *SHA-0*, *SHA-1*, *SHA-2*, and *SHA-3*.

SHA-1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols.

SHA-1 produces a 160-bit message digest based on principles similar to those used by Ronald L. Rivest of MIT in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design.

Simulation and Analysis

Existing schemes fail to protect all content of packets from attackers, so that the attacker can obtain information like packet type and sequence number etc. This information can be used to relate two packets, which break unlinkability and may lead to source trace back attacks.

In this project, an efficient privacy maintain routing protocol ASOR that achieves content unobservability by employing anonymous key establishment based on group signature is introduced. The setup of ASOR is simple: each node only has to obtain a group signature signing key and an ID-based private key from an offline key server as depicted in Fig 4.

Earlier a number of schemes have been proposed to protect privacy in Adhoc networks. However, none of these schemes offer complete unlinkability or unobservability since data packets and control packets are still linkable and distinguishable in these schemes.

1. Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.
2. Unlinkability of two or more IOIs means these IOIs are no more or no less related from the attacker's view.
3. Unobservability of an IOI is the state that whether it exists or not is indistinguishable to all unrelated subjects, and subjects related to this IOI are anonymous to all other related subjects.

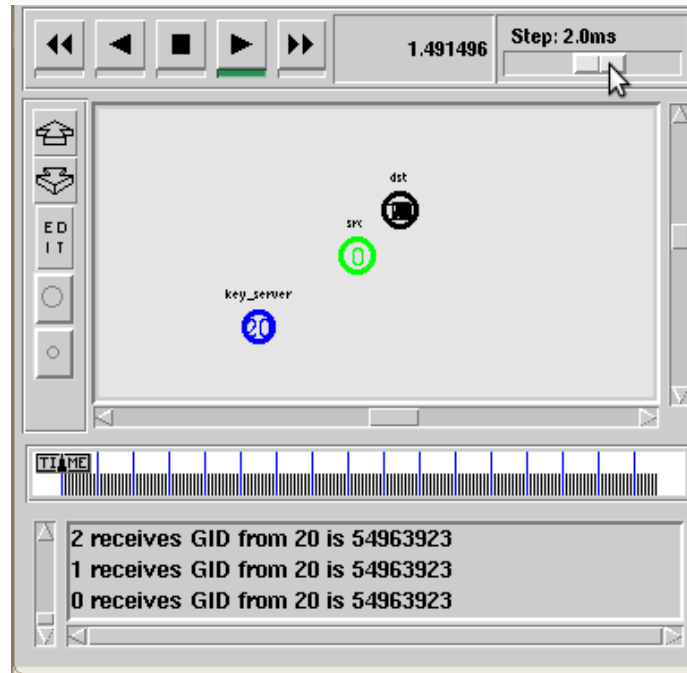


Figure 4: Key Server

Hence stronger privacy requirements regarding privacy-preserving routing in mobile ad hoc networks are defined. Then an Anonymous secure routing scheme ASOR is proposed to offer complete unlinkability and content unobservability for all types of packets.

Following protocols, which we are considered in this project

- AODV
- MASK
- ASOR

The simulation results show that ASOR not only has satisfactory performance compared to AODV, but also achieves stronger privacy protection than existing schemes like MASK.

In this protocol, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish routing packets and data packets from dummy traffic with inexpensive symmetric decryption. Table 1 shows the performance comparison with existing system.

Table 1: Performance Comparison

Protocol	PDF (%)	OH (pkt)	Delay (ms)
AODV	89.926	316	37
MASK	8	316	400
ASOR	82	183	38

1. Encryption and decryption procedures:

Each user has own encryption and decryption procedures, E and D, with the former in the public file and the latter kept secret. These procedures are related to the keys, which, in RSA specifically, are sets of two special numbers. We of course start out with the message itself, symbolized by M, which is to be “encrypted”. There are four procedures that are specific and essential to a public-key cryptosystem:

- a) Deciphering an enciphered message gives you the original message, specifically $D(E(M)) = M$
- b) Reversing the procedures still returns M: $E(D(M)) = M$
- c) E and D are easy to compute.
- d) The publicity of E does not compromise the secrecy of D, meaning you cannot easily figure out D from E.

With a given E, we are still not given an efficient way of computing D. If $C = E(M)$ is the cipher text, then trying to figure out D by trying to satisfy an M in $E(M) = C$ is unreasonably difficult: the number of messages to test would be impractically large.

An E that satisfies (a), (c), and (d) is called a “trap-door one-way function” and is also a “trap-door one-way permutation”. It is a trap door because since its inverse D is easy to compute if certain “trap-door” information is available, but otherwise hard. It is one-way because it is easy to compute in one direction, but hard in the other. It is a permutation because it satisfies (b), meaning every cipher text is a potential message, and every message is a ciphertext of some other message. Statement (b) is in fact just needed to provide “signatures”.

So far, we expect to make E and D easy to compute through simple arithmetic. We must now represent the message numerically, so that we can perform these arithmetic algorithms on it. Now let’s represent M by an integer between 0 and $n - 1$. If the message is too long, sparse it up and encrypt separately. Let e, d, n be positive integers, with (e, n) as the encryption key, (d, n) the decryption key, $n = pq$.

Now, we encrypt the message by raising it to the eth power modulo n to obtain C, the cipher text. We then decrypt C by raising it to the dth power modulo n to obtain M again. Formally, we obtain these encryption and decryption algorithms for E and D:

$$C \equiv E(M) \equiv M^e \pmod{n}$$

$$M \equiv D(C) \equiv C^d \pmod{n}$$

Note that we are preserving the same information size, since M and C are integers between 0 and $n - 1$, and because of the modular congruence. Also note the simplicity of the fact that the encryption/decryption keys are both just pairs of integers, (e, n) and (d, n). These are different for every user, and should generally be subscripted, but we’ll consider just the general case here.

Now the question of creating the encryption key itself. First, choosing two “random” large primes p and q, we multiply and produce $n = pq$. Although n is public, it will not reveal p and q since it is essentially impossible to factor them from n, and therefore will assure that d is practically impossible to derive from e.

Now we want to obtain the appropriate e and d . We pick d to be a random large integer, which must be co-prime to $(p - 1) \cdot (q - 1)$, meaning the following equation has to be satisfied:

We will want to compute e from d , p , and q , where e is the multiplicative inverse of d . That means we need to satisfy

$$e \cdot d = 1 \pmod{\phi(n)} .$$

which is equivalent to

$$e \cdot d = k \cdot \phi(n) + 1$$

for some integer k .

2. Signatures:

For complete assurance that the message originated from a sender, and was not just sent through him by a third party who may have used the same encryption key (that of the receiver), we need a digital signature to come with the message. This has obvious implications of importance in real-life applications.

Bob wants to send a private message to Alice. To sign the document, we pull a clever little trick, all assuming that the RSA algorithm is quick and reliable, mostly due to property (c). We decrypt a message with Bob's key, allowed by properties (a) and (b), which assert that every message is the cipher text of another message, and that every cipher text can be interpreted as a message. Formally,

$$DB(M) = S.$$

Then we encrypt S with Alice's encryption key.

$$EA(S) = EA(DB(M))$$

The highly secure performance of the proposed system is shown graphically in Fig 5.

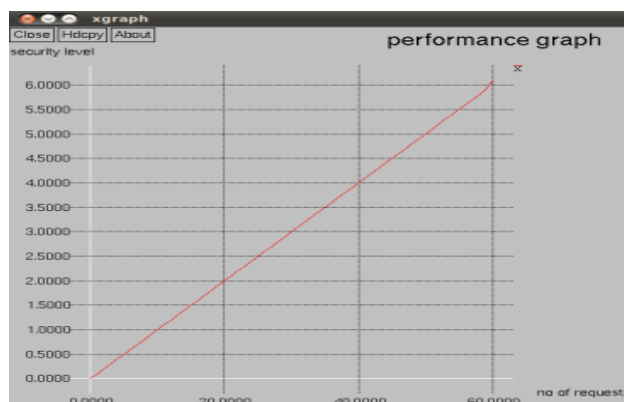


Figure 5: Simulation Waveform

Fig 6 shows the comparison graph of the proposed protocol with other existing protocols showing end to end delay which provides better results.

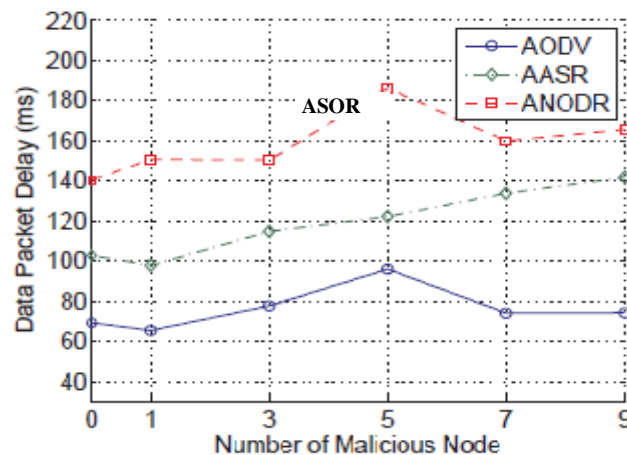


Figure 6: End to End Delay

Conclusion

An Anonymous routing protocol ASOR based on group signature and ID-based cryptosystem for ad hoc networks is proposed. The design of ASOR offers strong privacy protection—completes unlinkability and content unobservability for ad hoc networks. The security analysis demonstrates that ASOR not only provides strong privacy protection, it is also more resistant against attacks due to node compromise. The proposed method is tested with wormhole attack provided good performance with improved security data transmission. We implemented the protocol on ns2 and examined performance of ASOR, which shows that ASOR has satisfactory performance in terms of packet delivery ratio, latency and normalized control bytes.

References

- [1] J. Liu, F. R. Yu, C.-H. Lung, and H. Tang, "Optimal combined intrusion detection and biometric-based continuous authentication in high security mobile ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 2, pp. 806–815, Feb. 2009
- [2] F. R. Yu, H. Tang, S. Bu, and D. Zheng, "Security and quality of service(QoS) co-design in cooperative mobile ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2013, no. 1, pp. 188–190, July 2013
- [3] F. Li, Y. Yang, and J. Wu, "Attack and flee: game-theory-based analysis on interactions among nodes in MANETs," *IEEE Trans. Syst., Man, Cybern. (B)*, vol.40, pp.612–622, June 2010.
- [4] Shengrong Bu, P. Liu, and Helen Tang "Structural Results for Combined Continuous User Authentication and Intrusion Detection in High Security Mobile Ad-Hoc Networks", *IEEE Trans. Wireless Commun.*, vol. 10, issue9, sep2011.

- [5] Xiannuan Liang and Yang Xiao, "Game Theory for Network Security", IEEE Commun Surveys, vol. 15, issue1,2013.
- [6] Sanjay Kumar Suman, Dhananjay Kumar & Bhagyalakshmi, L 2014, 'Non Cooperative Power Control Game with new Pricing for Wireless Ad hoc Networks', International review on Computers and Software, vol. 9, no. 1, 18-28.
- [7] T.Alpcan and T. Basar, Network Security: A Decision and Game Theoretic Approach. Cambridge University Press,2010.
- [8] A.Patcha and J. M. Park, "A game theoretic formulation for intrusion detection in mobile ad hoc networks," Int'l J. Netw. Security, vol. 2, no. 2, pp. 131–137,2006.
- [9] Angelos Antonopoulos and Christos Verikoukis, "Multi-Player Game Theoretic MAC Strategies foR Energy Efficient Data Dissemination", IEEE Trans, Wireless Communs, Vol. 13, No. 2, Feb 2014
- [10] Fan Wang, Ossama Younis , Marwan Krunz, " Throughput-oriented MAC for mobile ad hoc networks:A game-theoretic approach", Ad Hoc Networks 7 (2009) 98–117
- [11] Sanjay Kumar Suman, Dhananjay Kumar & Bhagyalakshmi, L 2014, 'Review of Power Control Problem in Wireless Ad hoc Networks in Game Theoretic Perspective', Internal journal of advanced research in computer science and software engineering, vol. 4, no. 2, pp. 589-593.
- [12] H.Tembine, P. Vilanova, M. Assaad, and M. Debbah, "Mean field stochastic games for SINR-based medium access control," in Proc. 2011 Int'l ICST Conf. Performance Evaluation Methodologies Tools.
- [13] H. Zhang, O. Kreidl, B. DeCleene, J. Kurose, and X. Ni, "Security analysis of the bootstrap protocol for deny-by-default mobile ad-hoc networks," in Proc. 2009 MILCOM.
- [14] Dr. S.K. Mahendran, "Advanced Security Mechanism for Mobile Ad hoc Networks using Game Theoretic Approach", (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 5, June 2014
- [15] Sanjay Kumar Suman, Dhananjay Kumar & Bhagyalakshmi, L "SINR Pricing in Non Cooperative Power Control Game for Wireless Ad hoc Networks", KSII Transactions on Internet and Information System, vol8,no.7,pp.2281-2301
- [16] Verikoukis and Angelos Antonopoulos, " Multi-Player Game Theoretic MAC Strategies for Energy Efficient Data Dissemination" IEEE Trans. Wireless Commun., vol 13, NO. 2, Feb 2014
- [17] Lin Chen, and Jean Leneutre, "A Game Theoretic Framework of Distributed Power and rate control in IEEE 802.11 WLAN", IEEE Journal on Communs, Vol. 26, NO. 7, Sep 2008.
- [18] C.K. Tan M.L. Sim T.C. Chuah, "Game theoretic approach for channel and power control with no- internal - regret learning in wireless ad hoc Networks", IET Communications,

- [19] Long, Qian Zhang, Bo Li, Huilong Yang and Xiping Guan, “Non Cooperative Power Control for Wireless Adhoc Networks with Repeated Games”, IEEE Journal in Commnications Vol. 25, No. 6, Aug 2007.