International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 5 Issue 4 July 2015
International Manuscript ID : 2249054XV5I4072015-02

EFFECTIVE AND PRAGMATIC REVIEW ON THE SECURITY ISSUES IN THE ASSORTED NETWORKS

Shubham Rathi
M.Tech. Research Scholar
Computer Science and Engineering
Modern Institute of Engineering and Technology
Ambala, Haryana, India
E-mail : shubham.rathi88@gmail.com

Gagan Kumar
Assistant Professor
Computer Science and Engineering
Modern Institute of Engineering and Technology
Ambala, Haryana, India
E-mail : gagansoft@gmail.com

ABSTRACT

The wireless network is currently having number of attacks and threats from multiple directions. Now days, an advancement in the wireless networks is done in the form of Internet of Things (IoT) that is a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has evolved from the convergence of wireless technologies, micro-electromechanical systems (MEMS) and the Internet. A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low -- or any other

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 5 Issue 4 July 2015
International Manuscript ID : 2249054XV5I4072015-02

natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network. So far, the Internet of Things has been most closely associated with machine-to-machine (M2M) communication in manufacturing and power, oil and gas utilities. Products built with M2M communication capabilities are often referred to as being smart. In this research work, we have proposed and implemented a unique multilayered algorithm for high level security in the scenario of IoT

Keywords – Network Security, IoT Security, Network Key Exchange

INTRODUCTION

Wireless communication is getting the notoriety a tremendous and heaps of fame among the clients now days and this is chiefly because of the innovative insurgency in the field of cell telephones, laptops, PDA, remote LAN and modems. There are two separate ways to create the correspondence among various hosts:

First technique is to use a current cell pecking request which passes on data and also voice; in the phone system, there is a consolidated association or a settled base station which handles coordinating and resource organization routines, since all the directing decisions are made in a bound together way. Therefore these systems are similarly called Infrastructural based systems. Nevertheless the essential issue here is handoff between two zones when customer moves from one cell to other. It transforms into a discriminating to trade data quickly while handoff. Another guideline issue is that it is obliged to the zone where system is accessible.

In the second approach we can structure an impromptu system among all clients who needs to relate with one another. This proposes all the clients in the astoundingly designated system must be on edge to forward information packs to affirm that the packs are gone on from the source to destination. This sign of systems association is more minute than the cell framework and just

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 5 Issue 4 July 2015
International Manuscript ID : 2249054XV5I4072015-02

obliged in the reach by the individual focuses transmission range. This framework has its own particular perfect circumstances over cell structure and these are:

i. On the interest setup

ii. Tolerance towards deficiency

iii. Unconstrained network

In programming building and information exchanges, the wireless sensor frameworks are an element examination area with different workshops and joins engineered consistently, for occurrence IPSN and SenSys.

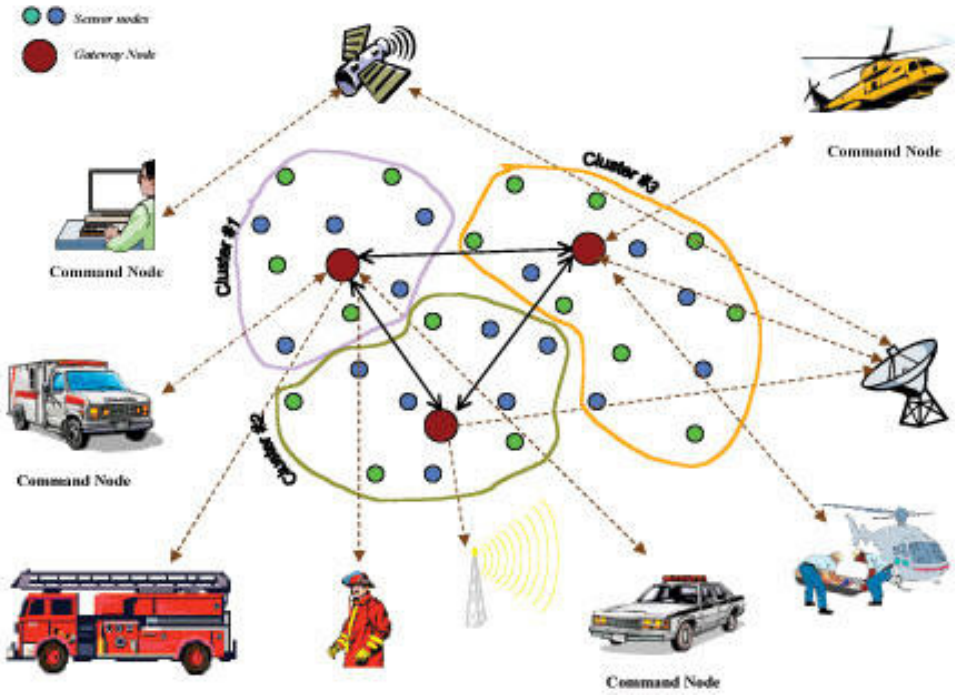

Figure 1.1 – Wireless Sensor Networks and IoT Association

The key attributes of wireless sensor networks include:

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 5 Issue 4 July 2015
International Manuscript ID : 2249054XV5I4072015-02

- Utilization of power imperatives for hubs utilizing power devices or vitality reaping
- Capacity to adapt to hub disappointments (strength)
- Versatility of hubs
- Heterogeneity of hubs
- Versatility to huge size of sending
- Capacity to withstand cruel natural conditions
- Convenience
- Cross-layer outline

Cross-layer is changing into a principal focusing on area for remote exchanges. Also, the routine layered approach displays three central issues:

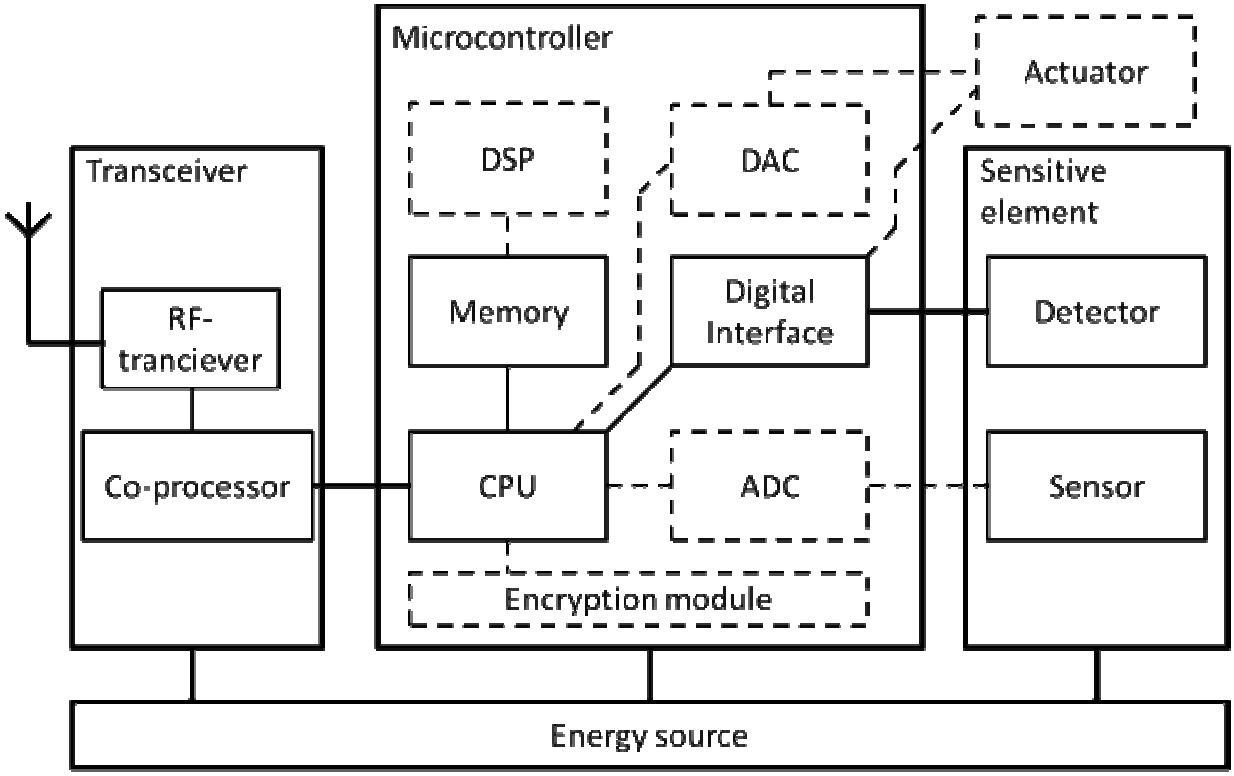

Figure 1.2 – Components of a typical Wireless Sensor Node

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 5 Issue 4 July 2015
International Manuscript ID : 2249054XV5I4072015-02

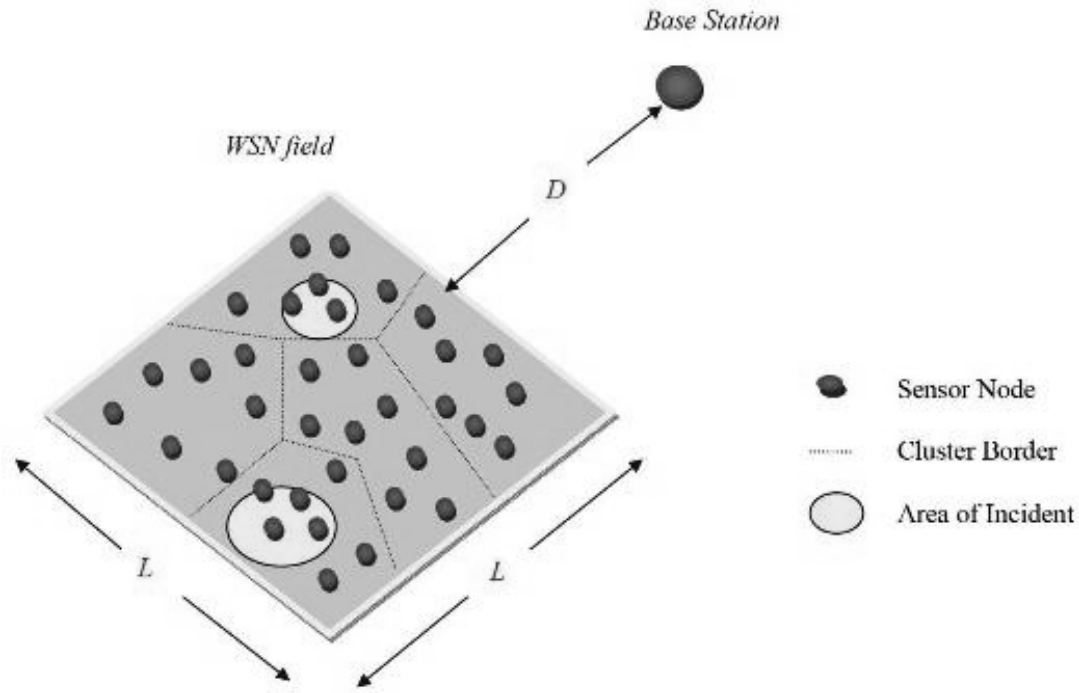

Figure 1.3 : Classical Format of WSN Node

Regular layered framework can't offer assorted information among gathered layers , which prompts every one layer not having complete information. The basic layered structure can't guarantee the development of the entire structure.

The standard layered rationale does not can adjust to the natural change.

Working frameworks for remote sensor system focuses are routinely less entangled than by and large profitable working structures. They all the more firmly take after installed structures, for two reasons.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 5 Issue 4 July 2015
International Manuscript ID : 2249054XV5I4072015-02

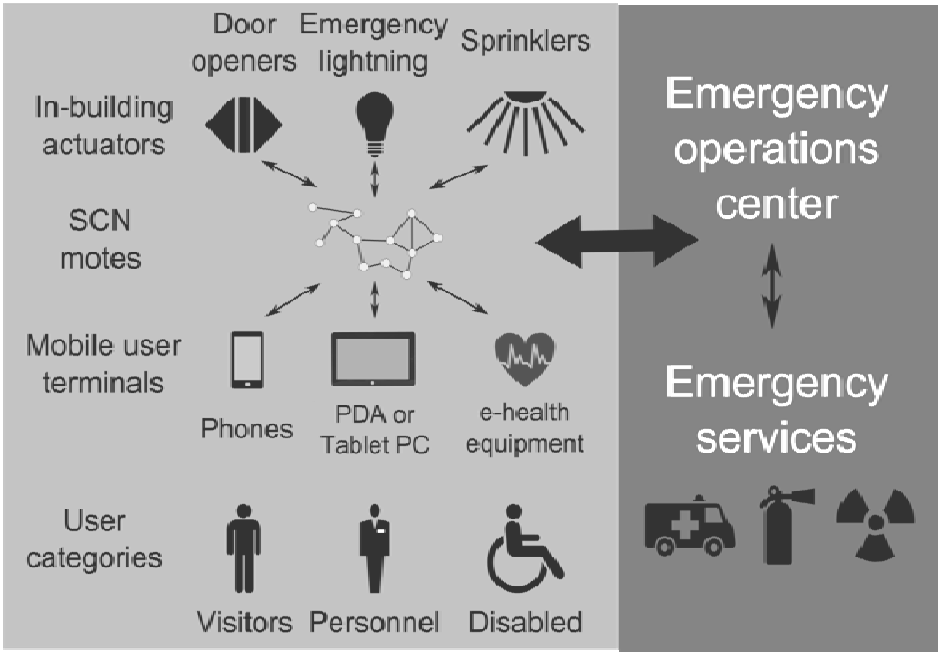

Figure 1.4 – Wireless Sensor Networks in medical domain

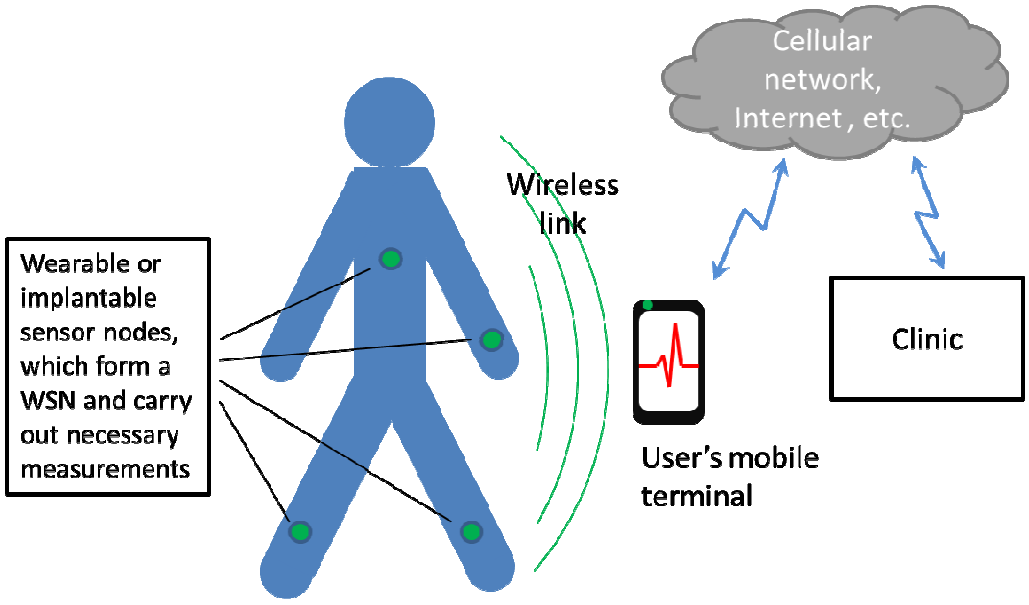

Figure 1.5 – RFID and WSN in Medical and Health Sciences

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 5 Issue 4 July 2015
International Manuscript ID : 2249054XV5I4072015-02

Open key concepts are in light of test issues which beginning now surrender no fit blueprint that are inborn in certain whole number factorization, discrete logarithm, and elliptic turn affiliations. It is computationally direct for a client to convey their own particular open and private key-pair and to utilize them for encryption and disentangling. The quality lies in the way that it is "amazing" (computationally infeasible) for a fittingly made private key to be absolutely driven from its relating open key. In this way general society key may be appropriated without managing security, however the private key must not be uncovered to anybody not attested to investigate messages or perform pushed engravings. Open key estimations, not under any condition like symmetric key figurings, don't oblige a safe fundamental trade of one (or more) puzzle keys between the get-together.

Advanced marks are oftentimes used to realize electronic marks, a more far reaching term that implies any electronic data that passes on the objective of a mark, yet not all electronic marks use computerized marks. In a couple of countries, including the United States, India, Brazil, and people from the European Union, electronic marks have real significance.

Advanced marks use a kind of hilter kilter cryptography. For messages sent through a nonsecure channel, a properly executed computerized mark gives the beneficiary inspiration to acknowledge the message was sent by the ensured sender.

In various cases, typical with engineering associations for case, computerized seals are furthermore required for a substitute layer of endorsement and security. Computerized seals and marks are similar to physically composed marks and stamped seals. Advanced marks are equivalent to customary translated marks in various respects, however suitably executed computerized marks are more difficult to create than the deciphered sort. Computerized mark plans, in the sense used here, are cryptographically based, and must be realized honestly to be

influential. Computerized marks can in like manner give non-refusal, inferring that the guarantor can't viably attest they didn't sign a message, while moreover ensuring their private key stays puzzle; further, some non-renouncement arrangements offer a period stamp for the advanced mark, so paying little respect to the likelihood that the private key is revealed, the mark is true blue. Digitally stamped messages may be anything representable as a bitstring: cases fuse electronic mail, contracts, or a message sent through some other.

LITERATURE SURVEY

To propose and defend the research work, a number of research papers are analyzed. Following are the excerpts from the different research work performed by number of academicians and researchers.

Roberto Di Pietro (2003) - This paper describes a probabilistic model and two protocols to establish a secure pair-wise communication channel between any pair of sensors in the WSN, by assigning a small set of random keys to each sensor. We build, based on the first Direct Protocol, a second Co-operative Protocol. The Co-operative Protocol is adaptive: its security properties can be dynamically changed during the life-time of the WSN. Both protocols also guarantee implicit and probabilistic mutual authentication without any additional overhead and without the presence of a base station. The performance of the Direct Protocol is analytically characterized while, for the Co-operative Protocol, we provide both analytical evaluations and extensive simulations. For example, the results show that, assuming each sensor stores 120 keys, in a WSN composed of 1024 sensors with 32 corrupted sensors the probability of a channel corruption is negligible in the case of the Co-operative Protocol.

David Wagner (2004) – This paper introduce TinySec, the first fully-implemented link layer security architecture for wireless sensor networks. In our design, we leverage recent lessons learned from design vulnerabilities in security protocols for other wireless networks such as 802.11b and GSM. Conventional security protocols tend to be conservative in their security guarantees, typically adding 16--32 bytes of overhead. With small memories, weak processors,

limited energy, and 30 byte packets, sensor networks cannot afford this luxury. TinySec addresses these extreme resource constraints with careful design; we explore the tradeoffs among different cryptographic primitives and use the inherent sensor network limitations to our advantage when choosing parameters to find a sweet spot for security, packet overhead, and resource requirements. TinySec is portable to a variety of hardware and radio platforms. The experimental results on a 36 node distributed sensor network application clearly demonstrate that software based link layer protocols are feasible and efficient, adding less than 10% energy, latency, and bandwidth overhead.

Wenliang Du (2004) – This work propose a novel random key pre-distribution scheme that exploits deployment knowledge and avoids unnecessary key assignments. This work show that the performance (including connectivity, memory usage, and network resilience against node capture) of sensor networks can he substantially improved with the use of our proposed scheme. The scheme and its detailed performance evaluation are presented in this paper.

Wenliang Du (2005) - In this paper, the authors provide a framework in which to study the security of key predistribution schemes, propose a new key predistribution scheme which substantially improves the resilience of the network compared to previous schemes, and give an in-depth analysis of our scheme in terms of network resilience and associated overhead. The proposed scheme exhibits a nice threshold property: when the number of compromised nodes is less than the threshold, the probability that communications between any additional nodes are compromised is close to zero. This desirable property lowers the initial payoff of smaller-scale network breaches to an adversary, and makes it necessary for the adversary to attack a large fraction of the network before it can achieve any significant gain.

An Liu (2008) - This paper reports the experimental evaluation of TinyECC on several common sensor platforms, including MICAz, Tmote Sky, and Imotel. The evaluation results show the impacts of individual optimizations on the execution time and resource consumptions, and give the most computationally efficient and the most storage efficient configuration of TinyECC.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 5 Issue 4 July 2015
International Manuscript ID : 2249054XV5I4072015-02

Atzori, L., Iera, A., & Morabito, G. (2010) - This paper addresses the Internet of Things. Principle empowering component of this promising standard is the coordination of a few advancements and interchanges arrangements. Recognizable proof and following advances, wired and remote sensor and actuator systems, improved correspondence conventions (imparted to the Next Generation Internet), and appropriated insight for keen articles are only the most significant. As one can undoubtedly envision, any genuine commitment to the development of the Internet of Things must essentially be the aftereffect of synergetic exercises directed in diverse fields of learning, for example, information transfers, informatics, gadgets and sociology. In such an intricate situation, this review is coordinated to the individuals who need to approach this unpredictable train and add to its improvement. Diverse dreams of this Internet of Things standard are accounted for and empowering advancements audited. What rises is that still real issues should be confronted by the exploration group. The most pertinent among them are tended to in subtle elements.

Real Life Implementations and Applications of the Wireless Networks

From building and home automation to wearables, the IoT touches every facet of our lives. Many corporate giants including Texas Instruments, Cisco, Ericsson, Freescale, GE are working in the development as well as deployment of IoT scenarios. The companies are making and developing the applications easier with hardware, software and support to get anything connected within the IoT. A set of key markets exists for the IoT with potential for exponential growth.

- Medical and healthcare systems
- Building and home automation
- Transportation
- Wearables - Smart watch for Location and tracking
- Building & home automation
- Smart cities
- Smart manufacturing

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 5 Issue 4 July 2015
International Manuscript ID : 2249054XV5I4072015-02

- Employee safety
- Predictive maintenance
- Health care
- Remote monitoring
- Ambulance telemetry
- Drug tracking
- Hospital asset tracking
- Access control
- Automotive

CONCLUSION

The proposed measurement for the arrangement and enactment of the IoT hubs are novel regarding higher security on the human association end, still the use metaheuristic strategies including hereditary calculation, ground dwelling insect state advancement and neural systems can give ideal results as far as more noteworthy security and uprightness. A different pile of conventions and methods are utilized for fulfilling the undertaking of security and protection in WSNs. Be that as it may, the proposed work is actualized with an extraordinary arrangement of errands and steps. There are number parameters or measurements which are needed be considered for the mix and investigation of security angles.

REFERENCES

[1] T.H Clausen, “Introduction to Mobile Ad-hoc Networks (MANET)” , 2007.

[2] “Wi-Fi (wireless networking technology)” Encyclopaedia, 2002.

[3] Che-Fn Yu, “Security safe guards for intelligent networks”, GTE laboratories incorporated, 40 sylvan road, Waltham, MA 02254.

[4] V. Venkata Ramana, Dr. A. Rama Mohan Reddy, and Dr. K. Chandra Sekaran, "Bio Inspired Approach to Secure Routing in MANETs", International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3, No.4, July 2012

[5] Sun Choi, Doo-young Kim, Do-hyeon Lee, Jae-il Jung, "WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks", International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, IEEE, 2008.

[6] Tuna Guven, Hui Zeng, Jason H. Li, Song Luo, Subir Das, Tony McAuley, Thomas Stuhrmann, Joe Sherrick, Christine Adelfio, Seth Spoenlein, Aristides Staikos, Mario Gerla, "A Multi-Layer Approach For Seamless Handoff In Ad Hoc Networks With Wireless Heterogenity", IEEE, Paper ID 900668.pdf.

[7] D.Suresh kumar, K.Manikandan, M.A.Saleem Durai, "Secure On-Demand Routing Protocol for MANET using Genetic Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 19– No.8, April 2011.

[8] S.Prasad, Y.P.Singh, and C.S.Rai,"Swarm Based Intelligent Routing for MANETs", International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[9] Poonam Garg,"A Comparison between Memetic algorithm and Genetic algorithm for the cryptanalysis of Simplified Data Encryption Standard algorithm", International Journal of Network Security & Its Applications (IJNSA), Vol.1, No 1, April 2009

[10] Lu Han, Dongming Zhaow, and Manli Zhou, "A Network Layer Security Mechanism Based on Collaborative Intelligent Agents in MANET" IEEE,2005

[11] Santhosh Krishna B.V, Mrs.Vallikannu A.L, "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism", International Journal of Scientific & Engineering Research, Volume 1, Issue 3, December-2010

[12] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", international conference on wireless networks, 2003

[13] Marek Hejmo, Brian L. Mark, Member, IEEE, Charikleia Zouridaki, Student Member, IEEE, and Roshan K. Thomas, "Design and Analysis of a Denial-of-Service-Resistant Quality-of-Service Signaling Protocol for MANETs", IEEE Transactions On Vehicular Technology, Vol. 55, No. 3, May 2006

[14] Arif Sari and Dr. Beran Necat, "Securing Mobile Ad-Hoc Networks Against Jamming Attacks Through Unified Security Mechanism", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3, June 2012

[15] Ms. Neetu Singh Chouhan, Ms. Shweta Yadav. " Flooding Attacks Prevention in MANET", International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3

[16] Dimitris Mitropoulos and Diomidis Spinellis, "Securing e-voting against MITM attacks", 13th Panhellenic Conference on Informatics, Corfu, Greece, September 2009

[17] Latha Tamilselvan and Dr. V. Sankaranarayanan, "Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks", IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.3, March 2007

[18] Manel Guerrero Zapata, "Secure Ad hoc On-Demand Distance Vector Routing", Mobile Computing and Communications Review, Volume 6, Number 3.

[19] Dr. C. Anbalagan and Mr. T. Sugantha, "Implementation of Evolutionary Algorithms in Different Methods of Research- A Analytical Approach with Selection, Recombination, Mutation,

[20] Reinsertion and Population Model, IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), Vol.1, No. 1, October 2011

[21] Jason Leonard, "Interactive Game Scheduling With Genetic Algorithms", 1998

[22] Dr. James F. Smith III and Robert D. Rhyne II, "A Fuzzy Logic Algorithm For Optimal Allocation Of Distributed Resources".

[23] Manoj V, Mohammed Aaqib, Raghavendiran N and Vijayan R, "A Novel Security Framework Using Trust And Fuzzy Logic In Manet", International