International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-01

PRIVACY, DEFENCE AND CONFIDENTIALITY IN MOBILE AD-HOC NETWORKS IN ASSOCIATION WITH MULTIPLE ALGORITHMS

Bilal Riyadh Imran. (M.Tech)
CSE Department
M. M. Engineering College,
M. M. University,
Mullana, Ambala, Haryana, India-133207
engbilal219@yahoo.com

Rohit Vaid
CSE Department
M. M. Engineering College,
M. M. University,
Mullana, Ambala, Haryana, India-133207
rohit_vaid1@rediffmail.com

Abstract

Mobile Ad-hoc Network (MANET) is characterized as the moving hub as opposed to any altered framework, go about as a versatile switch. These portable switches are answerable for the system portability. The historical backdrop of portable system start after the concoction of 802.11 or wifi they are generally utilized for associating around themselves and for interfacing with the web by means of any altered foundation. Vehicles like auto, transports and trains furnished with switch goes about as settled Mobile Ad-hoc Network. Vehicles today comprises numerous implanted mechanisms like assemble in switches, electronic gadgets like Sensors PDAs raise in GPS, giving web association with it gives, data and infotainment to the clients. These developments in MANET helps the vehicle to correspond with one another, at the time of crisis like mischance, or throughout climatic progressions like snow fall, and at the time of barricade, this data will be educated to the adjacent vehicles. This paper highlights the security and secrecy issues connected with the portable specially appointed systems.

I. INTRODUCTION

Nowadays technologies rising to provide efficiency to MANET users like providing enough storage space, as we all know the cloud computing is the next generation computing paradigm many researches are conducting experiments on Mobile Ad-hoc Network to provide the cloud service securely.

Genetic algorithm is useful for providing optimization solution in various search related problems using the natural evolutionary techniques like

- Inheritance
- Mutation
- Selection
- Crossover

The main technique followed in genetic algorithm was among the group of people an individual has been selected to solve the optimization problem. The individuals, who have been selected among the group, should be fit for the mutation. Those individuals are mutated form next generation. After producing enough number of generations, this algorithm terminates automatically.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-01

WatchDog Technique

Watchdogs are the basis of dierent Intrusion Detection Systems. They have the advantage of using only lo cal information and therefore, they are robust to most of the attacks. Although imp ortance of this mechanism is clear, it is hard to nd studies that seriously test the watchdog in wireless mobile scenarios with high degrees of mobility, a characteristic of any Mobile Ad Hoc Network (MANET).

Confidant

Recently, an intrusion detection system which named CONFIDANT was proposed, which utilized file integrity analyzers and mobile agent for intrusion detection and aimed to detection of malicious activity by insiders. Shi et al proposed CONFIDANT has vulnerabilities in security aspect, so they integrated a clone agent protocol into CONFIDANT in 2009. Because of Shi et al's protocol's high communication cost, we proposed a new attribute-policy handshake structure for CONFIDANT to protect agents and strengthen its security even though there are a few malicious platforms.

Core

CORE (Collaborative Reputation): As nodes sometimes do not intentionally misbehave, i.e., battery condition is
low, these nodes should not be considered as misbehaving nodes and excluded from the network. To do this, the reputation
should be rated based on past reputation, which is zero (neutral) at the beginning. In addition, participation in the network
can be categorized into several functions such as routing discovery (in DSR) or forwarding packets. Each of these activities
has different level of effects to the network; for example, forwarding packets has more effect on the performance of the
system than that of routing discovery. Therefore, significance weight of functions should be used in the calculation of the
reputation.

OCEAN

Bansal and Baker [19] also proposed an extension on top of the DSR protocol called OCEAN (Observation-based Cooperation Enforcement in Adhoc Networks). OCEAN also uses a monitoring system and a reputation system. However, in contrast to the previous approaches above, OCEAN relies only on its own observation to avoid the new vulnerability of false accusation from second-hand reputation exchanges. Therefore, OCEAN can be considered as a stand-alone architecture. OCEAN categorizes routing misbehavior into two types: misleading and selfish. If a node has participated in the route discovery but not packet forwarding, this is considered to be misleading as it misleads other nodes to route packets through it. But if a node does not even participate in the route discovery, it is considered to be selfish.

2ack

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-01

2ACK scheme is used to detect the misbehaving nodes. It sends two hop acknowledgment packets in the opposite direction of the routing path. 2ACK scheme reduces additional routing overhead by acknowledging fraction of the received data packets. It uses the Dynamic Source Routing (DSR) protocol. The proposed 1ACK scheme try to reduce the overhead of Acknowledgments caused by 2ACK scheme

Cooperative

In modern era of technology wireless networks are widely used for data communication through out the world. Mobile Ad hoc Network (MANET) is one of the type in which each device works as an independent node and also as a router for forwarding data between nodes of the MANET. MANET has no centralized or authorized body to protect the communication from intruders and considered as vulnerable to attacks due to its distributed nature and lack of infrastructure. Cluster based distributed and cooperative intrusion detection system (IDS) provides security to some extent. The header node in a cluster is a key component because if compromised the whole cluster will be destroyed. We propose a system that uses two heads per cluster with cooperative IDS mechanism. These head nodes not only cooperate for finding intrusion for cluster members but also protect each other against intrusion. In result more permenent cluster will appear which give birth to more consistent network connection. The performance metric of our work is based on how smoothly and securely the cluster operates when one header is compromised. The proposed system increases the detection rate and decreases the traffic and therefore offers the efficient utilization of power in mobile nodes.

SORI

He, Wu and Kholsa [31] developed a system SORI, The Secure and Objective Reputation-based Incentive Scheme for ad hoc network focus on the packet forwarding function. It consists of three basic components: neighbour monitoring, reputation propagation and punishment. Each neighbours forwarding function is linked with two parameters S A B C D RFn(Request for forwarding) and HFn(x) (Has Forwarded). A Local Evaluation Record (LERn (x) is created using the values of RFn(x) and HFn(x) which depicts the confidence metric. The more the packet transmitted to x for forwarding, the higher the confidence about the trustworthiness of x. In this method, the nodes exchange reputation information only with their neighbours. A non cooperative node will be punished by its entire neighbour. Each node n periodically updates LERn(x) and the respective value of its neighbour to calculate OERn(x) (Overall Evaluation Record). If the OERn(x) is lower than a predefined threshold, node n takes p punishment action by probabilistically, that the node do not intentionally drop the packets, It takes no countermeasures to prevent collusion.

II. LITERATURE REVIEW

Impact of Denial of Service Solutions on Network Quality of Service, Scott Fowler 2013 - The Internet has become a universal communication network tool. It has evolved from a platform that supports best-effort traffic to one that now carries

different traffic types including those involving continuous media with Quality of Service (QoS) requirements. As more services are delivered over the Internet, the world face increasing risk to their availability given that malicious attacks on those Internet services continue to increase. Several networks have witnessed Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks over the past few years which have disrupted QoS of network services, thereby violating the Service Level Agreement (SLA) between the client and the Internet Service Provider (ISP). Hence DoS or DDoS attacks are major threats to network QoS. In this paper the authors survey techniques and solutions that have been deployed to thwart DoS and DDoS attacks and we evaluate them in terms of their impact on network QoS for Internet services. The authors also present vulnerabilities that can be exploited for QoS protocols and also affect QoS if exploited. In addition, the work also highlight challenges that still need to be addressed to achieve end-to-end QoS with recently proposed DoS/DDoS solutions.

An Improved Ant Colony Otimization (IACO) Based Multicasting in MANET, Deepender Dhull, Swati Dhull : A Mobile Ad hoc Network (MANET) is one of the challenging environments for multicast. Since the associated overhead is more, the existing studies illustrate that tree-based and mesh-based on-demand protocols are not the best choice. The costs of the tree under multiple constraints are reduced by the several algorithms which are based on the Ant Colony Optimization (ACO) approach. The traffic-engineering multicast problem is treated as a single-purpose problem with several constraints with the help of these algorithms. The main disadvantage of this approach is the need of a predefined upper bound that can isolate good trees from the final solution. In order to solve the traffic engineering multicast problem which optimizes many objectives simultaneously this study offers a design on Ant Based Multicast Routing (AMR) algorithm for multicast routing in mobile ad hoc networks. Apart from the existing constraints such as distance, delay and bandwidth, the algorithm calculates one more additional constraint in the cost metric which is the product of average-delay and the maximum depth of the multicast tree. Moreover it also attempts to reduce the combined cost metric. By reducing the number of group members that participate in the construction of the multicast structure and by providing robustness to mobility by performing broadcasts in densely clustered local regions, the proposed protocol achieves packet delivery statistics that are comparable to that with a pure multicast protocol but with significantly lower overheads. By this protocol we achieve increased Packet Delivery Fraction (PDF) with reduced overhead and routing load. By simulation results, it is clear that our proposed algorithm surpasses all the previous algorithms by developing multicast trees with different sizes.

I.

II. Wen-Hwa Liao (2011) - in the Paper entitled “Ant colony optimization based sensor deployment protocol for Adhoc Networks,’’ proposed an Sensor deployment is one of the most important issues in wireless sensor networks, because an efficient deployment scheme can reduce the deployment cost and enhance the detection

capability of the wireless sensor networks. In addition, it can enhance the quality of monitoring in wireless sensor networks by increasing the coverage area. Ant colony optimization (ACO) algorithm provides a natural and intrinsic way of exploration of search space for multiple knapsack problem (MKP). This work considers the problem of sensor deployment to achieve complete coverage of the service region and maximize the lifetime of the network. This work model the deployment problem as the multiple knapsack problem. Based on ACO algorithm, this paper proposed a deployment scheme to prolong the network lifetime, while ensuring complete coverage of the service region. The simulations show that the proposed algorithm can prolong the lifetime of the network.

III.

Xie, Meng (2011) in the Paper entitled "Ant-Colony Optimization Based In-Network Data Aggregation In Adhoc Networks, '' proposed an In-network data aggregation is an important technique in Adhoc Networks. It improves the security and alleviates congestive routing traffic by eliminating data redundancy in message passing processes. Ant-colony aggregation is a distributed algorithm that provides an intrinsic way of exploring search space to optimize settings for optimal data aggregation. This thesis aims to refine the heuristic function and the aggregation node selection method to maximize energy efficiency and extend network lifetime.

Secure on demand routing technique using Genetic Algorithm

Routing path is needed for the source and destination nodes connecting for the first time, by broadcasting RREQ message to the neighbouring nodes to find the destination node. If there is a route already established between source and destination.

III. ATTACKS IN MOBILE AD HOC NETWORKS

Having discussed the basic concept and the applications of MANETs, we look at some typical attacks in MANETs in this section. It is very important for protocol designers to keep in mind various attacks when designing the security mechanisms for MANETs

Attacks against MANETs can be roughly classified into two major categories, namely external attacks and internal attacks, according to the domain of attacks. External attacks are carried out by nodes that do not belong to the domain of the network. These attackers try to join the network and access the resources without authorization. Unlike external attacks, internal attacks are from compromised nodes, which are actually part of the network. Compared with external attacks, internal ones are more serious because the attackers know valuable and secret information from compromised nodes and possess privileged access rights to the network resources. Furthermore, some attacks could be launched at multiple layers of MANETs. We list some typical attacks in MANETs as follows: Eavesdropping: eavesdropping is a very easy passive attack in the wireless communication environment. By placing an antenna at an appropriate location, an attacker can intercept and read the sensitive information that the victim transmits or receives without attracting the victim's attention. However, this attack can usually be

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-01

prevented by encrypting the transmitted data. Traffic Monitoring and Analysis: Traffic monitoring and analysis can be deployed to collect information of network nodes and data transmission such as the identities and locations of nodes and the amount of data transmitted among them. These information could be exploited to launch further attacks. _ Routing Attacks: Attackers try to alter the routing information and data in the routing control packet. There are several attacks that fall into this category, such as rushing attacks and wormhole attacks. _ Location Disclosure Attack: Attackers attempt to reveal information regarding the location of nodes or the structure of the network. By gathering the nodes' location information, the attacker can know which nodes are located in the routing path to the target node, and then plan the further attacks. _ Resource Consumption Attack: In this attack a malicious node interacts with a victim with the intention of consuming its battery life by requesting excessive route discovery, or by forwarding unnecessary packets to that node.

IV. MEMETIC ALGORITHM

Memetic algorithm is used as an interaction of any population based approach for every individuals learning on their own. Memetic algorithm plays an important role in evolutionary computation. This algorithm is also named as evolutionary algorithm. According to Richard dawkins meme is the fundamental unit of cultural transmissions or replications. The term memetic came from the word meme. Meme represent the cultural changes apart from genetic changes.

Implementation of Memetic algorithm

This algorithm produces several solutions for a single problem at hand. These solutions are entitled as individual in Evolutionary algorithm terminology. These solutions are treated to show similar behaviour during corporate assistance and competition, to make everyone accept they are from same species.

Fuzzy logic

Fuzzy logic is a multi valued technique, it is proposed by lotif zade in the year of 1965. Fuzzy logic manages approximate reasoning rather than unchanging and exact prediction. Fuzzy logic uses the binary values like 0 and 1 as the variables, to predict the results. Fuzzy logic technique provides approximate solutions to the unclear data or partial data.

Fuzzy logic degree of truth

Fuzzy logic is mathematically similar to the probabilistic logic, but fuzzy logic differ from probabilistic logic only based on truth values like 0 and 1, fuzzy logic related to degree of truth, whereas probabilistic logic corresponds to probability prospects.

Types of fuzzy logics

There are several types of fuzzy logic as per mathematical logic, they are

- Relative fuzzy logic
- Predicate fuzzy logic

Relative fuzzy logic

The significant relative fuzzy logics are

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-01

- Monoidal t-norm predicate relative fuzzy logic
- Fundamental relative fuzzy logic
- Lucasiewicz relative fuzzy logic

Monoidal t-norm predicate relative fuzzy logic

Monoidal t-norm predicate relative fuzzy logic is maximization logic in this left incessant t norm defines the combinations and residuum of t-norms defines the suggestion. Monoidal t-norm predictive algebra related to this model.

The left incessant t norms is defined as

$$u * v \leq w \text{ if and only if } u \leq (v \rightarrow w)$$

The residuum of left incessant t norms are defined as

$$u \rightarrow v = \sup\{w | w * u \leq v\}$$

This equation promotes residuum is the largest function for all u and v

$$u * (u \rightarrow v) \leq v$$

The residuum of left in cession t norms can be determined as the feeble function it makes fuzzy logic model as legitimate

Fundamental relative fuzzy logic

Fundamental relative fuzzy logic is the extension of monoidal t-norm predicate fuzzy logic, in this the combinations are denoted as residuum of t-norm, fundamental relative fuzzy logic is related to the fundamental relative fuzzy logic algebra.

Lucasiewicz fuzzy logic

Lucasiewicz fuzzy logic is the extension of fundamental relative fuzzy logic. It has the adage of basic fuzzy logic as well as adage of double negotiation. Lucasiewicz model includes the fundamental relative fuzzy logics.

Godel fuzzy logic

Godel fuzzy logic is the fundamental relative fuzzy logic, it has the combination of Lucasiewicz fuzzy logic as well as the adage of combination, and its models are called G- algebra.

Invent fuzzy logic

It is also the extension of fundamental relative fuzzy logic, it has the combination of invent fuzzy logic and another adage of eliminate combination, and its models are called invent algebras.

Predicate fuzzy logic

Predicate fuzzy logic widens the above mentioned fuzzy logics by including worldwide and existential identifiers in this manner the propositional logic creates the predicate logic. The terminology of worldwide identifier is Infimum in the t-norm fuzzy logic

Infimum is also called as infima.

Artificial neural network

An artificial neural network is an interconnection of nodes, like neurons connected to the brain. A neural network consists of many artificial neurons with interconnected groups, it process the information using the psychology approach to the calculation. Neural systems have the adaptive character so that it can change its structure during the learning phase. Neural networks are used to

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-01

design a complex relationship between input and output data. The neural networks are inspired from exploratory central nervous system. In artificial neural network the artificial nodes are connected to each other to form a network. Neural network models in artificial intelligence are referred as artificial neural network. It is usually defined by the function

$$f = U \rightarrow V$$

Sometimes it is associated with some rules or particular algorithms. Artificial neural networks are used for defining the class functions.

Network function

Network refers to interconnections between neurons, suppose consider a network consist of five levels the first level is the input, second, third and fourth level are the senders and the fifth level is the output neurons.

Artificial neural networks consists of three parameters

- The interconnection prototype between different levels of the neurons.
- The learning procedure for updating the weights of the interconnections.
- The activation neuron function converts the neurons biased input to its output commencement.

The network function $f(s)$ is defined from work of other functions $ni(s)$, this expediently represented as network structure, the extensively used type of work is the non linear weighted sum, where

$$f(s) = C(\sum_i wini(s))$$

C = activation function

$ni =$ Vector

There are two types of views in artificial neural networks

- First view or fundamental view
- Second view or probabilistic view

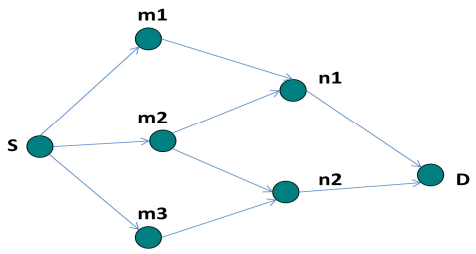

Figure 1 : Artificial dependency graph

First view or fundamental view

The input S is transformed into a 3-dimensional vector m, which is then transformed into a 2 dimensional vector n, which is finally transformed into D. This type of view is commonly encountered as optimization.

Second view or probabilistic view

The random variable $F = f(N)$ depends upon the random variable$N = n(M)$, which depends upon$M = m(S)$, which depends upon the random variable S. this is most commonly known as graphical models.

Erudition paradigms

There are three major erudition paradigms, each corresponding to a particular abstract erudition task. These are

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-01

- Supervised erudition
- Unsupervised erudition
- fortification erudition

Supervised erudition

In the supervised erudition, the example pairs $(u, v), u\epsilon U, v\epsilon V$. The aim is to find the function $f: U \rightarrow V$, the cost functions relate to the mismatch between the mapping and its data and also contains proceeding to the knowledge of the problem domain.

The jobs that fall within the hypothesis of the supervised erudition are pattern detection and deterioration. The supervised erudition concept is suitable to chronological data.

Unsupervised erudition

In unsupervised erudition, some data s is given and the cost of the function is diminished, that can be any function of the data s and the system's output f.

The outlay task is dependent on the function and the a priori hypothesis, for the insignificant example, consider the model

$$f(s) = a$$

Where $a =$ constant

Cost $C = E[(s - f(s))^2]$

$x =$ Mean of the data

The outlay function is the more complex. So it is applicable only based on the application, in firmness it is connected to the common information between s and $f(s)$. In the numerical modelling, it could be related to the posterior prospect of the model of the given data. The chores that fall within the prospect of unsupervised erudition are in general evaluation predicament.

Reinforcement erudition

In reinforcement erudition, data s are not given by an agent actually, but it is generated by agent relations with environment, the main objective is to analyze the minimizing technique for the long term cost.

The background dynamics of the long term cost is not known, but it is predictable. The background is modelled as markov decision process with the states $s1, s2, sn \epsilon S$ and their actions are represented as $a1, a2 \ldots am \epsilon A$

Arithmetic neural networks are often used in reinforcement erudition as a part of on the whole algorithm.

Algorithm for artificial neural network

- First step is to instruct the network according to the required data.
- Classify the problems, each input corresponds to a unique value and each output is a class value.
- The ultimate aim of this approach is to encode the network by creating n-dimensional credence space.
- The network is represented by simply enumerating each connection.

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 4 Issue 3 May 2014
International Manuscript ID : 2249054XV4I3052014-01

- Usually there will be more than one output class value for input value.

Behaviour based robotics

Behaviour robotics is the division of robotics which incorporates behavioural artificial intelligence. The behaviour based robotics was first discovered by professor Rodney brooks and their students in MIT.

Artificial intelligence robotics

In conventional the artificial intellect robotics is sequential dispensation units.

The main technique behind this artificial intelligence robotics is

- Illustration, interpretation and development
- Representation of structure
- Practical disintegration, hierarchical systems
- Figure management

The actions based approach defines that intelligence is obtained from interaction among the synchronous environment. The main ideas after this approach are

- Personification
- Evolving complications
- Improper planning

Behaviour

Behaviour is defined as reaction to stimulus. This process is most often seen in the automatic machine all over the world, it responds to every kind of actions.

Table 1: Comparison of Technique Proposed for Detecting Selfishness in MANET

Technique	**Self to Neighbor**	**Neighbor to Neighbor**	**Selfish Routing**	**Malicious Routing**	**Punishment**	**Avoid Misbehaving Node in route finding**
Watchdog	Y	N	N	N	Y	Y
Ex Watchdog	Y	Y	N	Y	Y	Y
Confidant	Y	N	Y	Y	Y	Y
CORE	Y	N	Y	Y	n	N
OCEAN	Y	Y	Y	N	Y	Y
2ACK	Y	Y	Y	Y	Y	Y
CO OPERATIVE IDS	Y	Y	Y	Y	NA	NA
SORI	Y	Y	Y	Y	Y	Y

V. CONCLUSION

In this manuscript, different security aspects of mobile ad hoc networks are highlighted. There are number of intrusion detection systems available in the existing work. In the proposed and future work, a unique and effective algorithmic approach shall be devised for combating against the malicious

traffic attack on mobile ad hoc networks. As conclusion, the major attacks and vulnerabilities on the MANETs are ddos, Sybil, wormhole, blackhole and many others. In the future work, the effective algorithm shall be used to detect and avoid the attacks.

REFERENCES

[1] Tomas Krag and Sebastian Büettrich (2004-01-24). "Wireless Mesh Networking". O'Reilly Wireless Dev Center. Retrieved 2009-01-20.

[2] Ma, Yajie; Richards, Mark; Ghanem, Moustafa; Guo, Yike; Hassard, John (2008). "Air Pollution Monitoring and Mining Based on Sensor Grid in London". Sensors 8 (6): 3601. doi:10.3390/s8063601. edit

[3] Ma, Yajie; Guo, Yike; Tian, Xiangchuan; Ghanem, Moustafa (2011). "Distributed Clustering-Based Aggregation Algorithm for Spatial Correlated Sensor Networks". IEEE Sensors Journal 11 (3): 641. doi:10.1109/JSEN.2010.2056916. edit

[4] Kleinrock, Leonard (1975). "Packet Switching in Radio Channels: Part I--Carrier Sense Multiple-Access Modes and Their Throughput-Delay Characteristics".

[5] Shi, Zhefu; Beard, Cory; Mitchell, Ken (2008). "Tunable traffic control for multihop CSMA networks".

[6] Kahn, R. E. (January 1977). "The Organization of Computer Resources into a Packet Radio Network". IEEE Transactions on Communications COM-25 (1): 169–178.

[7] Jubin, J., and Tornow, J. D. (January 1987). "The DARPA Packet Radio Network Protocols". Proceedings of the IEEE 75 (1).

[8] N. Schacham and J. Westcott (January 1987). "Future directions in packet radio architectures and protocols". Proceedings of the IEEE 75 (1): 83–99. doi:10.1109/PROC.1987.13707.

[9] Royer, E., Toh, C. (April 1999). "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks". IEEE Personal Communications 6 (2): 46–55. doi:10.1109/98.760423.

[10] Mauve, M., Widmer, J., Hartenstein, H. (December 2001). "A Survey on Position-Based Routing in Mobile Ad Hoc Networks". IEEE Network 1 (6): 30–39. doi:10.1109/65.967595.

[11] Maihöfer, C. (2nd quarter 2004). "A Survey on Geocast Routing Protocols". IEEE Communications Surveys and Tutorials 6 (2).

[12] Security issues, challenges & solution in MANET, IJCST Vol. 2, Issue 4, Oct . - Dec. 2011 ISSN : 0976-8491 (Online) | ISSN : 2229-4333(Print)

[13] International Journal of Artificial Intelligence & Applications (IJAIA), Vol.3, No.4, July 2012 DOI : 10.5121/ijaia.2012, Bio Inspired Approach to Secure Routing in MANETs, V. Venkata Ramana, Dr. A. Rama Mohan Reddy, and Dr. K. Chandra, Sekaran

[14] Black Hole Attack in Mobile Ad Hoc Networks, Mohammad Al-Shurman and Seong-Moo Yoo, Electrical and Computer Engineering Department, The University of Alabama in Huntsville, Huntsville, Alabama., Seungjin Park, Department of Computer Science, Michigan Technological University, Houghton, Michigan, Journal of Engineering Science and Technology, Vol. 4, No. 2 (2009) 243 - 250, School of Engineering, Taylor's University College

[15] Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks, Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, Department of Computer Science, IACC 258, North Dakota State University, Fargo

[16] Different Types of Attacks on Integrated MANET-Internet Communication, Abhay Kumar Rai, Department of Electronics & Communication, University of Allahabad, International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3) 265

[17] Nidhi Nigam et al , International Journal of Computer Science & Communication Networks,Vol 2(4), 531-535, A comprehension on Wormhole Attack prevention technique using THREADS in MANET, Nidhi Nigam, Vishal Sharma, Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology (COIT-2008), RIMT-IET, Mandi Gobindgarh. March 29, 2008