International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 10 Issue 1 –OCTOBER 2014.

A Congestion Attack in Selective Secure Mechanism Using Manet

V. Jeevitha[*1], and S. Kumaravel[#2]

[*]*Research Scholar, Mahendra Arts and Science College, Kalippatti., Namakkal (DT), Tamilnadu*

[#] *HOD (Computer Science), Mahendra Arts and Science College, Kalippatti., Namakkal (DT), Tamilnadu*

Abstract*— A wireless sensor networks (WSNs) pledge many new enthuse applications in the future, as ubiquitously on-demand multiply ascendancy, continual connectivity, and instantaneously deployable communication for armed and responders. These types of wireless sensor networks already help to observe critical environmental conditions in volcanic eruption areas, underwater and so on; factory maintenance works, and troop utilization, to name a few applications. As WSNs grow to be a greater extent essential to the everyday performance of people and organizations and also many attacks arise in the wireless ad hoc networks. The wireless intermediate is constantly subjected to deliberate intervention attacks in the networks such as jamming attacks. This paper argues about the downside of vampire or malevolent attack in the network routing path, and it is one of the most important attacks in the Ad hoc networks. This routing attack is complicated to recognize in the networks and this type attack destroys the properties of the routing protocols in the networks. Due to the introverted vampire attack in the wireless networks, total energy goes losing and escort to the entire networks to the crumple. In order to detect the vampire attacks in the wireless networks, this paper proposed the effectual protocol is serviceable during the packets are forwarded from server to client. And also we proposed the most effective technique to localize the sensor nodes in the wireless ad hoc networks. This technique is proposed for to localize the nodes in the networks in an accurate manner by using the real valued negative selection in routers. Although these negative consequences in the wireless networks, we illustrate two positive consequences that in the angle information is very useful. The angle information is not enough to obtain the overall geometry of the nodes. Angle information is satisfactory for a topology organize in the wireless networks.. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.

***Keywords*— Denial of service in the wireless networks, security analysis, routing protocol, wireless ad hoc networks, wireless sensor networks, wireless networks, fault node discovery, networks force, entire networks life.**

I. INTRODUCTION

A fundamental characteristic [1] of wireless ad hoc networks is the time difference of the channel potency of the original communication links. Such time difference occurs at numerous occasion scales and can be owing to multipath desertion, pathway loss using space attenuation, shadowing by obstacles, and intrusion from extra users. The impact of such time difference in the design of wireless ad hoc networks permeates throughout the layers, ranging from coding and power control at the physical layer to cellular hand off and coverage planning at the networking layer. An important means to cope with the time variation of the channel is the use of diversity. The basic design is to recover the presentation by creating numerous autonomous signal ways flanked by the source and the target nodes. These diversity modes pertain to a point-to-point link. Recent results point to another form of diversity, inherent in a wireless network with multiple users. Overall system throughput is maximized by allocating at any time the common channel resource to the user that can best exploit it. Similar results can be obtained for the downlink from the base station to the mobile users.

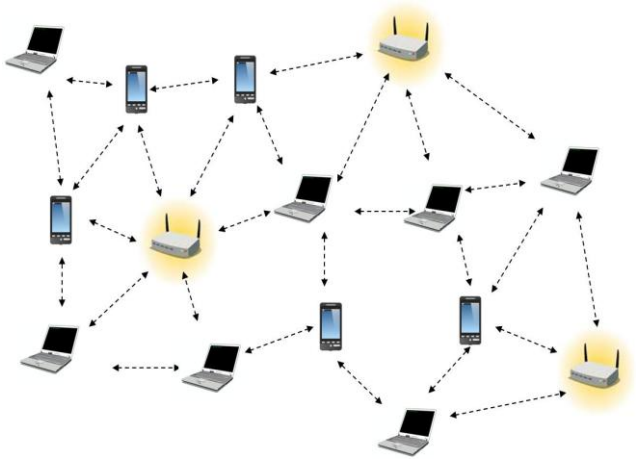


Fig-1 Architecture of Wireless Ad Hoc Networks

A Wireless ad hoc wireless sensor networks (WSNs) assuring many new exciting applications in the future, such an everywhere on-demand computing supremacy, incessant connectivity, and instantaneously deployable communication for armed and responders. These types of wireless sensor networks already help to observe critical environmental conditions in volcanic eruption areas, underwater and so on; factory maintenance works, and troop utilization, to name a few applications. As WSNs grow to be a greater extent essential to the everyday performance of people and organizations and also many attacks are arise in the wireless ad hoc networks.

In this paper, we are going to discuss about the actions of the vampire attacks in the wireless ad hoc networks. These types of attacks not directly link with the protocols; its links to the properties of the routing protocols in the communication networks. This attack affects the properties such as relation state between the nodes, remoteness vectors between the nodes, resource and location based routing. The vampire attack in the WSN is not easy to discover and to predict. Due to the solitary vampire attack in the networks, total force goes down and leads to the complete systems to the collapse. The vampire attacks can be classified has two types. There are: one is Carousel attack and another is Stretch attack.

In the Carousel attack, attackers introduce some packet within a route tranquil as a sequence of loops, such that the same node appears in the route of communication many times.

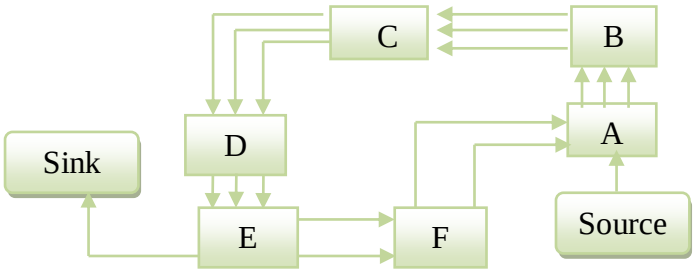


Figure 2 carousel attacks

This attack increases the routing length and delay very much in the networks and also inadequate by the number of allowable entries in the resource route.

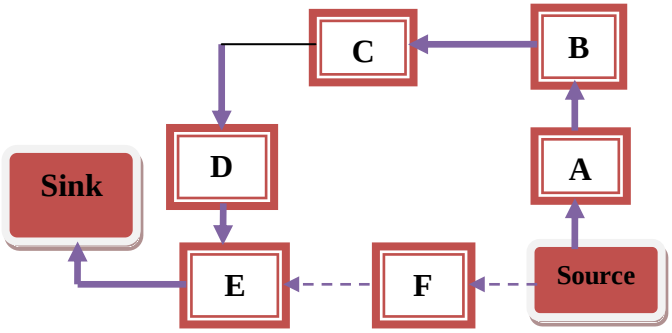


Fig 3 stretch attack dotted line indicates the malicious route

And the other attack also targeting resource steering, attackers construct falsely long routes, potentially traversing every node in the network. And also stretch attack, increases packet lane length, causing packets to be processed by a number of nodes that is self-governing of hop count down the straight path stuck between the challenger and packet target.

This routing attack is complicated to recognize in the networks and this type attack destroys the properties of the routing protocols in the networks. Due to the introverted vampire attack in the wireless networks, total energy goes losing and escort to the entire networks to the crumple. In order to detect the vampire attacks in the wireless networks, proposed the effectual protocol is serviceable during the packets are forwarded from server to client. And also proposed the most effective technique to localize the sensor nodes in the wireless ad hoc networks. This technique is proposed for to localize the nodes in the networks in an accurate manner by using the real valued negative selection in routers. Although these negative consequences in the wireless networks, we illustrate two positive consequences that in the angle information is very useful. The angle information is not enough to obtain the overall geometry of the nodes. Angle information is satisfactory for a topology organize in the wireless networks. It is NP-hard to find a valid embedding of a unit disk graph. On the positive side we'll show that by local angle information we can find a planar spanner sub-graph whose embedding in the plane can be used for geographical routing with guaranteed delivery. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.

The rest of the paper will be organized as follows: In section 2, we see about the related works of the paper. In section 3, we discuss about the proposed method. The algorithms and simulation are shown in the section 4 and 5. The conclusion of our paper is in section 6.

II. Related Works

In this section, let us see some of the related works to the intrusion detection of vampire in the wireless ad hoc networks using different approaches:

Matthias Grossglauser and David N. C. Tse [1], the capability of ad hoc wireless networks is forced by the common intrusion of concomitant communication between the two nodes. We study a model of a wireless ad hoc network where nodes correspond in arbitrary to the resource–target pairs. These wireless nodes are tacit to be mobile for the communication networks. We examine the each and every session throughput for the wireless network applications with variable stoppage constraints, such a wireless network

topology changes or clear in excess of the instant scale of packet or data's delivery. Under this statement, the per-user throughput can augment radically when nodes are movable moderately than fixed. This development can be achieved through by exploiting an appearance of multiuser multiplicity via sachet or information relaying between the two different nodes.

Shuo Guo, Ziguo Zhong and Tian He [2], wireless Sensor Networks are typically huge compilation of sensor nodes for cumulative of data or information as of watching the surroundings and broadcast to base position through multi-hop wireless message of nodes. The present of faults nodes in the WSNs are extremely lofty owing to wireless contact and unsystematic operation strategy. Force protection in wireless sensor network is an extra issue is to get better applicability of WSNs (wireless sensor networks). In order to overcome the above issues, we recommend division based misbehavior nodes identify and revival technique, which is as well as energy knowledgeable. In the above proposed technique, sensor nodes are agreed into several clusters. Cluster start and wireless sensor nodes are together for perceiving the fault in the sensor nodes. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.

B. Umakanth and J. Damodhar [3], Wireless Sensor Networks came to importance approximately the bargain of this millennium provoked by the ubiquitous situation of small-sized sensors with limited range control deployed in the huge information over a vicinity to examine different occurrence. The solitary motivation of a large segment of investigating efforts has been to exploit the lifetime of the wireless network, where network lifetime is typically measured from the immediacy of consumption to the peak when one of the nodes has exhausted its partial power source and become in-operational – normally referred since the first node collapse. In excess of the time, research has increasingly adopted ideas from wireless communications. In this paper, we consider how routing protocols, affect from attack even those designed to be protected, be short of security from these attacks, which we call Vampire attacks in the wireless networks, which permanently immobilize networks by quickly misbehavior nodes' of draining the sequence energy. These types of "parasite" attacks are not specific to any specific protocol which are overwhelming, not easy to identify, and are easy to bring out using as few as one wicked insider sending only procedure acquiescent messages. We proposed an EWMA method to bind the damage caused by these vampire types of attacks during the packet forwarding phase.

Zinaida Benenson, Peter M. cholewinski and, Felix C. freiling [4], We examine how wireless ad hoc networks can be attacked in follow. Beginning of this, we extend our previous idea of generic rival model that allows classifying the adversaries according to the two extents of power: presence and intervention. Thus, we provide a framework for realistic safety measures analysis in wireless sensor or ad hoc networks

Chris Karlof and David Wagner [5], we examine the routing protocol security in wireless networks. Many wireless sensor network routing protocols comprise be proposed in previous, but nothing of them have been considered with security as a goal in the wireless networks. We propose the effective protection goals for routing protocols in the sensor networks, show how attacks beside ad-hoc and end to end networking can be adapted into dominant attacks against sensor networks, initiate two classes of novel attacks touching sensor networks —sinkholes and HELLO floods, and we analyze that the security of all the major sensor network routing protocols. We illustrate crippling attacks against all of them and propose countermeasures and aim for considerations. This is the first such examine of secure routing in wireless sensor networks.

Farhad Nematy, and Naeim Rahmani [6], in modern years there has been a growing consideration in wireless ad hoc sensor networks (WSN) applications. Such wireless sensor networks are able to be second-hand to manage temperature in the desert or volcanic regions, humidity, contamination, pollution, etc. Energy utilization and dependability are two serious issues in WSNs. Faults or misbehavior occurring to sensor nodes is frequent owing to be short of power or ecological intrusion. In this paper recovery of faults nodes or misbehavior in cluster beginning deliberate and genetic system is used to recuperate huddle members to other cluster heads. Our Simulation results show the effectiveness that the proposed genetic algorithm can recover the fault nodes efficiently.

Dr. G. Padmavathi, and Mrs. D. Shanmugapriya, [7], Wireless Sensor networks (WSN) is a rising technology and have immense credibility to be betrothed insignificant situation like battlefield surveillance, marketable applications such as construction, travel examination, environment monitoring and well-groomed homes and several additional scenarios. Smart environments correspond to the subsequent evolutionary expansion rung in building our homes, utilities, manufacturing purposes, residence, shipboard, and shipping systems mechanization. Similar to several conscious creatures, the elegant surroundings rely initial and leading on sensory data or information as of the genuine humanity. Such a Sensory data or information comes as of numerous sensors of unlike modalities in scattered surroundings. The elegant atmosphere desires in order about its environment because, well about its interior mechanism; so it is captured in natural systems by the dissimilarity among the one is ext-receptors and other is pro-prioceptors. In the wireless communication

technologies also acquire various types of security intimidation. This paper deals with an extensive diversity of attacks or privacy issues in WSN and their categorization techniques and applying dissimilar security levels available to feel them as well as the challenges or issues faced in WSN.

Chaudhari H.C. And Kadam L.U [8], however, wireless sensor networks pretense exclusive protection challenges. Security is fetching a major anxiety for WSN protocol designers as of the extensive security serious applications of WSNs protocols. We include completed an attempt to document all the recognized security issues in wireless sensor networks and discuss a deal with an extensive diversity of attacks or privacy issues in WSN and their categorization techniques and applying dissimilar security levels available to feel them as well as the challenges or issues faced in WSN. In this paper, we took up the challenge or issues in the security level and have proposed an included wide-ranging security that will present security services for all services of the sensor network. The sensing technology shared with processing control and wireless communication makes it gainful for being broken in great measure in the future. The wireless communication technologies also acquire various types of security intimidation.

III. PROPOSED WORK

In this paper, we are going to discuss about the actions of the vampire attacks in the wireless ad hoc networks. These types of attacks not directly link with the protocols; its links to the properties of the routing protocols in the communication networks. This attack affects the properties such as relation state between the nodes, remoteness vectors between the nodes, resource and location based routing. The vampire attack in the WSN is not easy to discover and to predict. Due to the solitary vampire attack in the networks, total force goes down and leads to the complete systems to the collapse. The vampire attacks can be classified has two types. There are: one is Carousel attack and another is Stretch attack.

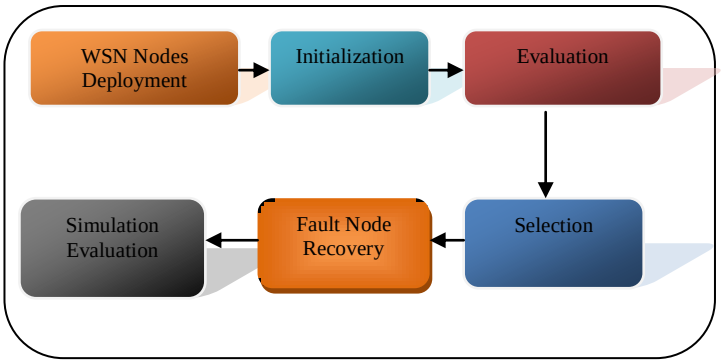
In order to overcome the above attacks in the wireless ad hoc networks, we proposed efficient protocol for secured transmission in the networks. And also we proposed the most effective technique to localize the sensor nodes in the wireless ad hoc networks. This technique is proposed for to localize the nodes in the networks in an accurate manner by using the real valued negative selection in routers. Although these negative consequences in the wireless networks, we illustrate two positive consequences that in the angle information is very useful. The angle information is not enough to obtain the overall geometry of the nodes. Angle information is satisfactory for a topology organize in the wireless networks. We propose an embedding algorithm with local angle information that gives surprisingly good results. We first formulate the embedding problem by a linear program with relaxed constraints such that any valid embedding must be a feasible solution to the LP. Through simulations, we show that the LP finds an almost identical set of locations as the original ones, even when the graph is sparse. We also show that the method is robust to both noisy measurements of angles and different models of sensor networks. Our proposed techniques are effective and efficient when compared to the previous approaches through our experimental and simulation analysis.

.

IV. ALGORITHM

Step1: Start WSN node deployment
Step 2: Initiate Grade diffusion process
Step 3: Sensor Node detects Event
Step 4: If backtracking
Step 5: Initialization process
Step 6: Evaluation process
Step 7: Selection process
Step 8: Crossover process
Step 9: Mutation process
Step 10: Then Data transmission
Else
Step 11: Data transmission

V. SIMULATION WORKS/RESULTS



1. Initialization:

In the initialization step, the genetic algorithm generates chromosomes, and each chromosome is an expected solution. The number of chromosomes is determined according to the population size, which is defined by the user. Each chromosome is a combined solution, and the chromosome length is the number of sensor nodes that are depleted or nonfunctioning. The elements in the genes are either 0 or 1. A

1 means the node should be replaced, and a 0 means that the node will not be replaced.

2. Evaluation:

In general, the fitness value is calculated according to a fitness function, and the parameters of the fitness function are the chromosome's genes. However, we cannot put genes directly into the fitness function in the FNR algorithm, because the genes on the chromosome are simply whether the node should be replaced or not. In the FNR algorithm, the goal is also to reuse the most routing paths and to replace the fewest sensor nodes. Hence, the number of routing paths available if some nonfunctioning sensor nodes are replaced is calculated.

3. Selection:

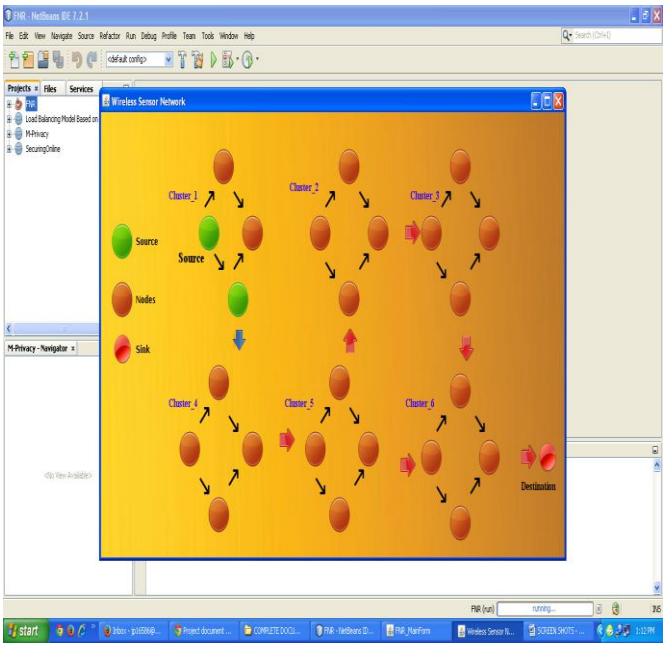
The selection step will eliminate the chromosomes with the lowest fitness values and retain the rest. We use the elitism strategy and keep the half of the chromosomes with better fitness values and put them in the mating pool. The worse chromosomes will be deleted, and new chromosomes will be made to replace them after the crossover step.

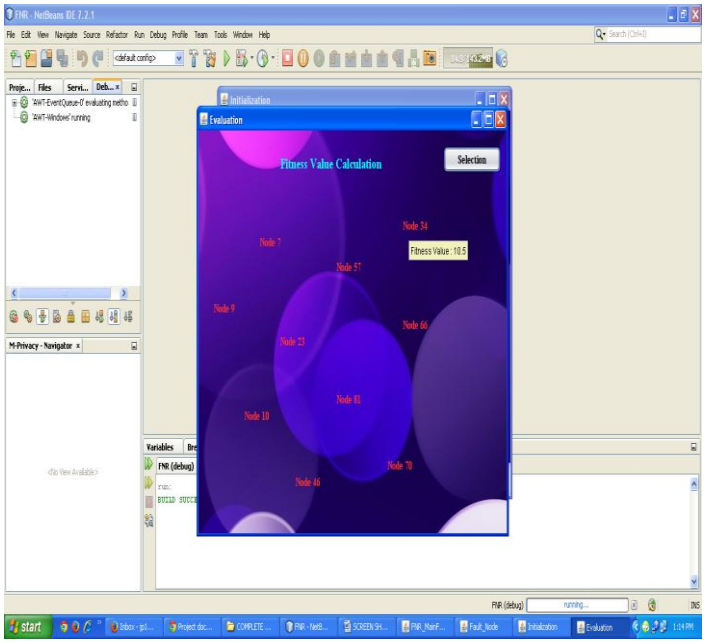
4. Crossover:

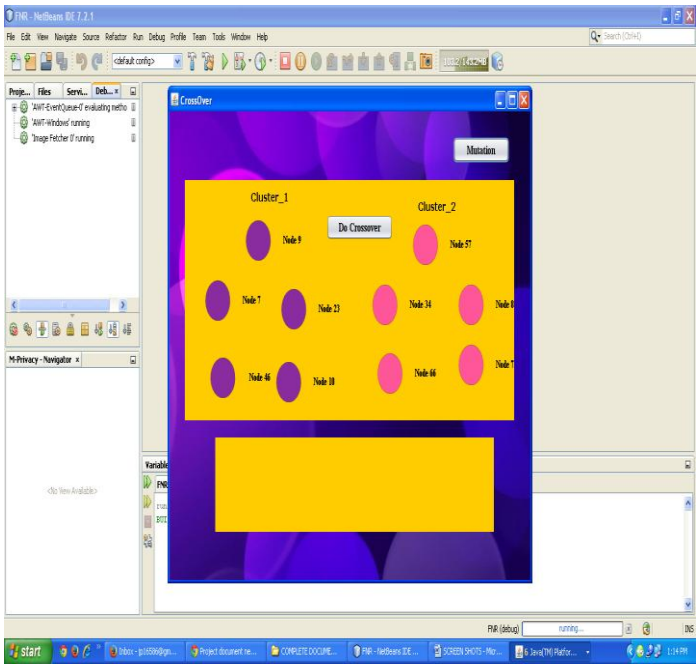
The crossover step is used in the genetic algorithm to change the individual chromosome. In this algorithm, we use the one-point crossover strategy to create new chromosomes. Two individual chromosomes are chosen from the mating pool to produce two new offspring. A crossover point is selected between the first and last genes of the parent individuals. Then, the fraction of each individual on either side of the crossover point is exchanged and concatenated. The rate of choice is made according to roulette-wheel selection and the fitness values.

5. Mutation:

The mutation step can introduce traits not found in the original individuals and prevents the GA from converging too fast. In this algorithm, we simply flip a gene randomly in the chromosome The chromosome with the best fitness value is the solution after the iteration. The FNR algorithm will replace the sensor nodes in the chromosome with genes of 1 to extend the WSN lifetime.







VI. CONCLUSION

Our proposed techniques in this paper, address the properties of routing protocol attacks in the wireless ad hoc networks In order to overcome the vampire or malicious attacks in WSN, the information transmission is carried in the trusted path of the networks. Our proposed technique addresses the vampire attacks in the wireless ad hoc networks when compared to the existing approaches. In the vampire attack, the two types of attacks may arisen the entire networks into collapse, total energy consumption level increases, and allocates long routing path and so on. And the two types of attacks are: In the Carousel attack, attackers introduce some packet within a route tranquil as a sequence of loops, such that the same node appears in the route of communication many times and the other attack is stretch attack also targeting resource steering, attackers construct falsely long routes, potentially traversing every node in the network. And also stretch attack, increases packet lane length, causing packets to be processed by a number of nodes that is self-governing of hop count down the straight path stuck between the challenger and packet target. This attack increases the routing length and delay very much in the networks and also inadequate by the number of allowable entries in the resource route. In this paper, we also proposed new technique to detect the misbehavior nodes in the wireless ad hoc networks by using the fault node detection technique. Our experimental result showed that our proposed novel technique works efficiently when compared to previous methods.

VII. REFERENCES

[1] Matthias Grossglauser and David N. C. Tse “Mobility Increases the Capacity of Ad Hoc Wireless Networks”- IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 10, NO. 4, AUGUST 2002

[2] Shuo Guo, Ziguo Zhong and Tian He “FIND: Faulty Node Detection for Wireless Sensor Networks”- SenSys’09, November 4–6, 2009, Berkeley, CA, USA

[3] B. Umakanth and J. Damodhar “Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks”- International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 8- August 2013.

[4] Zinaida Benenson, Peter M. cholewinski and, Felix C. freiling “Vulnerabilities and Attacks in Wireless Sensor Networks”

[5] Chris Karlof and David Wagner proposed “Trust Evaluation Based Security Solution in Ad Hoc Networks”

[6] Farhad Nematy , and Naeim Rahmani “A New Approach for Recovering Nodes from Faulty Cluster Heads Using Genetic Algorithm”- Proceedings of the International Conference on Soft Computing for Problem Solving (SocProS 2011) December 20-22, 2011

[7] Dr. G. Padmavathi, and Mrs. D. Shanmugapriya “Simulation of a Secure Ad Hoc Network Routing Protocol”- (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009

[8] Chaudhari H.C. And Kadam L.U “Security in Ad Hoc Networks”- International Journal of Networking Volume 1, Issue 1, 2011, pp-04-16.

[9] I. Aad, J. -P. Hubaux, and E.W. Knightly, “Denial of Service Resilience in Ad Hoc Networks,”Proc. ACM MobiCom, 2004.

[10] G. Ac's, L. Buttyan, and I. Vajda, “Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks,”IEEE Trans. Mobile Computing, Vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[11] T. Aura, “DoS-Resistant Authentication with Client Puzzles,”Proc. Int’l Workshop Security Protocols,2001.

[12] J. Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,”Proc. 12th Conf. USENIX Security, 2003.

[13] D. Bernstein and P. Schwabe, “New AES Software Speed Records,”Proc. Ninth Int’l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.

[14] D.J. Bernstein, “Syn Cookies,” http://cr.yp.to/syncookies.html,1996.

[15] I.F. Blaked, G. Serossi, and N.P. Smart, Elliptic Curves in Cryptography,vol. 265. Cambridge Univ., 1999.

[16] J.W. Bos, D.A. Osvik, and D. Stefan, “Fast Implementations of AES on Various Platforms,” Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.

[17] H. Chan and A. Perrig, “Security and Privacy in Sensor Networks,”Computer,vol. 36, no. 10, pp. 103-105, Oct. 2003.

[18] J.-H. Chang and L. Tassiulas, “Maximum Lifetime Routing in Wireless Sensor Networks,”IEEE/ACM Trans. Networking,vol. 12, no. 4, pp. 609-619, Aug. 2004.

[19] T.H. Clausen and P. Jacquet,Optimized Link State Routing Protocol (OLSR),IETF RFC 3626, 2003.

[20] J. Deng, R. Han, and S. Mishra, “Defending against Path-Based DoS Attacks in Wireless Sensor Networks,”Proc. ACM Workshop Security of Ad Hoc and Sensor Networks,2005.

[21] J. Deng, R. Han, and S. Mishra, “INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks,”Computer Comm.,vol. 29, no. 2, pp. 216-230, 2006.

[22] S. Doshi, S. Bhandare, and T.X. Brown, “An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network,”ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.