Journal of Theoretical and Applied Information Technology
15th January 2018. Vol.96. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

PROTECTING INVULNERABILITY AND SECURITY FOR WIRELESS SENSOR NETWORKS TO SAVE DATA

V.KRISHNA[#1] SYED UMAR [#2], O.RAMESH[#3] N. YOGENDER NATH [#4]

[#1] Assist .Professor, Department of Computer Science Engineering, MLR Institute of Technology, Hyderabad

[#2] Professor, Department of Computer Science Engineering, MLR Institute of Technology, Hyderabad

[#3] Assist .Professor, Department of Computer Science Engineering, MLR Institute of Technology, Hyderabad

[#4] Assist .Professor, Department of Computer Science Engineering, MLR Institute of Technology, Hyderabad

ABSTRACT

Based on the wireless sensor networks many applications are developed where more usage at military, medical fields. All this leads to exposure of the network against various threats from the outside. The network security from external attacks considered as one of the most important studies of today. This study examined the effects of security limits the wireless network WSN, typical attacks of certain species, and provided security over the years for a wide range of emotions to detect attacks and to protect wireless network.

Keywords: *WSN, Self-Defence, Authentication, Security*

1. INTRODUCTION.

The widespread use of wireless networks to see how the temperature monitoring sensor, easy to use and control the battlefield of enemies, and field etc., light. The network consists of thousands of injuries and, creates aliases environments and open, there are some external network threats and attacks. [1]. Some regulatory processes and algorithms in the field, but not complete protection against network attacks and intrusions. In sensor networks, wireless security requirements for privacy into account when designing the security system. We can identify independent systems require sensors and wireless links (WSN), to accept the use of effects that occur in the system when exposed to attacks from outside. All network effects, which are as follows: Each incoming packet, the fragmentation, neighbours, transmitter unit, RTS threshold, a strong signal is received and process costs.

1.1. Storage WSN

Editor is not a good environment wireless network and wireless transmission without property, and the information on an important part of WSN. The security (authentication, integrity, confidentiality, flexibility and self-organization) is very important WSN [2].

1. Recognition: A Review of WSN send existing customers.
2. Data integrity to ensure that the same information during transmission, some of the key safety
3. The resolution is a powerful security and destruction.
4. The exchange is an important requirement for the safety of the protocol design effective and efficient routing of WSN. The change means that believe that there is no communication with the growth of the network increase. add the network. [3]
5. Since the deployment of sensors and wireless networks in different environment and own forms of self-organization. [4].

1.2. Limitations of WSN

Wireless networks are many information and limitations [5] internal (storage, processing and transmission of the network links, etc.,) [6] Unlike other networks, security algorithms are considered. These limits [7-8-9]:

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

- The influence and network transmission.
- Random topology.
- effect.
- Distribution.
- Fault Tolerance
- The connection to the surrounding environment.
- Animals.

1.3. The Importance of information

See detection to detect consistently on the network or series of events to monitor the attacks and abnormal, damaging the cardiac damage security work on the methods and protection against attacks. [10] The cognitive process cognitive systems building divided two types:

Anomaly detection: In this category, a system or network, and general practice, primary care database, the country store to see the difference. The research in this area, based on [11] [12] cluster, data extraction, vaccines [15] Multi-media [13], neural networks, Support Vector Machine (SVM) [14], the model hidden Markov [16].Is included in the category of the immune system a lawsuit against network attacks using penetration measures like the current system: Two-way detection. Types of systems, methods, technology experts based static transfer analysis, conceptual design, technology, etc.

1.4. Literature Survey

From [1], consider that routing security in WSN, existing routing protocols have been proposed on communication from one node to other and none of them are concentrate on the security while transferring the data in between the nodes. In [16-20] proposed a new security goal for routing in sensor networks. It helps to analyse the data and how security is maintained while transferring data in between the nodes in which includes energy saving topology based algorithms in fig 1

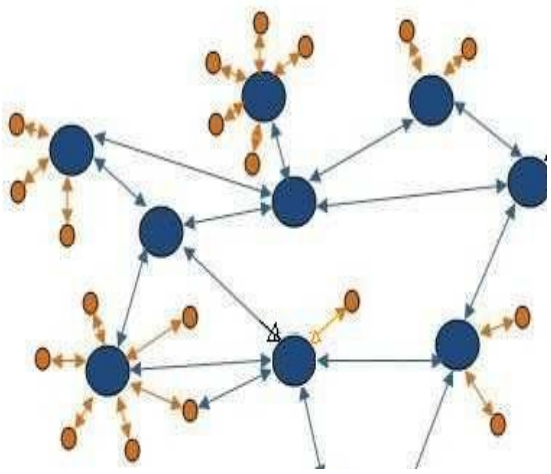

Fig:1 Security In WSN

Wireless sensor network is highly vulnerable to attacks because it consists of various resourceconstrained devices with their low battery power, less memory, and associated low energy. Sensor nodes communicate among themselves via wireless links. However, there are still a lot of unresolved issues in wireless sensor networks of which security is one of the hottest research issues. Sensor networks are deployed in hostile environments. Environmental conditions along with resource-constraints give rise to many type of security threats or attacks. Securely communication among sensor nodes is a fundamental challenge for providing security services in WSNs. This paper gives the security of wireless sensor network and attack at different layered architecture of WSN and their prevention.

2. PROTECTION MECHANISM:

Fenders hanging deviate. cluster topology network topology, see Figure 1.

Journal of Theoretical and Applied Information Technology
15th January 2018. Vol.96. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

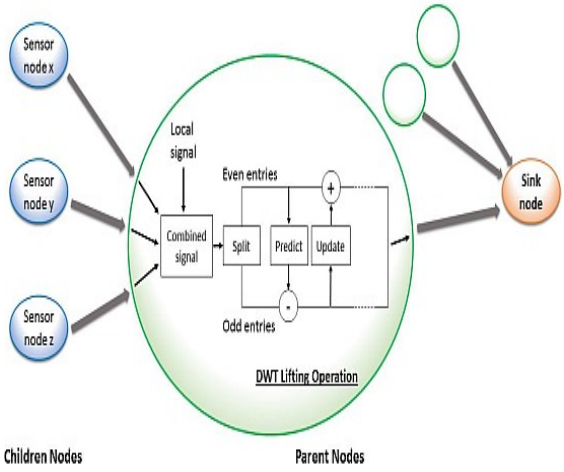

Figure 1.1: Clustering Of WSN Nodes

Explain some key points that it is:

- The protection device to the base station.
- Add all the data classes concern directly to the base station.
- Each node in the cluster to send their data only for the brush cluster.
- This function sets the base station, a great source and capable of communicating with each node of the brush. It can protect the device for the network:known attack (abnormal behaviour of the obtained attacks are known), for example:
- collision attacks, unfair competition, exhaustion attacks, an optional sinkhole, Sybil, wormholes and Hi Flood.
- advanced,unknown attacks (abnormal behaviour before attacking the result is not known): if the device works, including self-learning phase, which would explain later.
- Pager like the functioning of the brain, the brain retrieves the data from the body and detects abnormal behaviour based on the information in the brain and other details of purchase data. As shown in Figure 2.

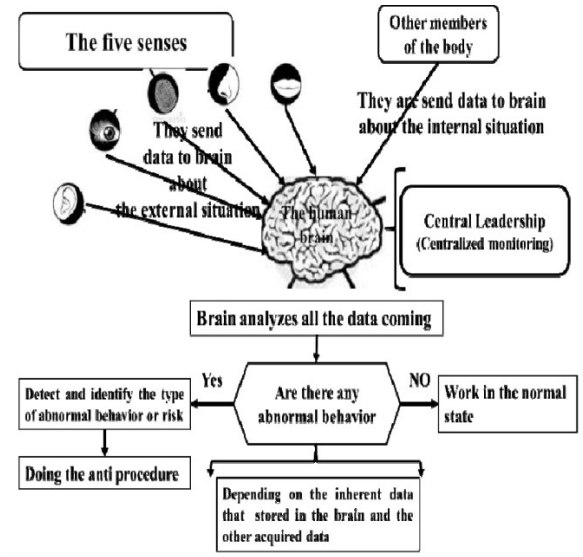

Figure 2: Brain Functionality With All Senses

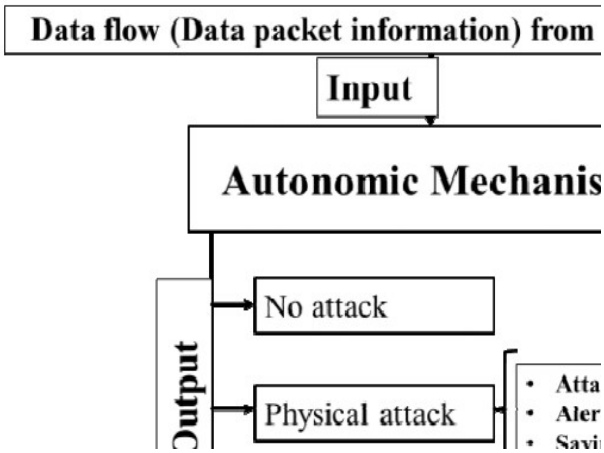

Figure 3: Data Flow Of Working Pattern From NH.

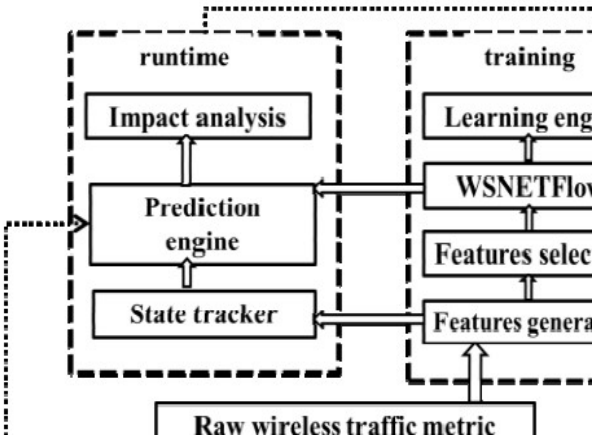

Figure 4: Mechanism For Protection Of WSN

Journal of Theoretical and Applied Information Technology
15th January 2018. Vol.96. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Protection mechanism is composed of four elements:

2.1. Collection and Processing Of Data

The natural state of the network set up the bank of the characteristics of the network device data when operating in its natural state, without any attack[21]. The database contains information such as latency, packet delivery, packet collisions caused average data studies in the interval time arrival rate processes of RTS packets caused e-Packet nearby Number Packet Delivery and signal strength, etc. At this stage, the average value for each property will be equal to the above calculation, and for a certain period (t).

To create the end of this phase, you obtain the following Table 1 and Table 2 and Table 3, and at the end of this phase, the backup unit of the data, if necessary[22-25].

Cluster heads IDs	Packet Delivery Waiting Time	Packet Collision Ratio	Average Time of Sending Packet Interval	RTS Packet Arrival Rate	Packet Drop Ratio	Packet Delivery ratio
ID1						
.						
IDr						

Table 1: Collection Of Data

Network Nodes	Coun
Node0_ID	
Node1_ID	
Node2_ID	

Table 2: Number Of Nodes

Network Nodes	Packet D
Node0_ID	
Node1_ID	
Node2_ID	

Table 3: Packet Delivery Signal Strength.

2.2. Analysis Of Attacks

In this phase, the processing device algorithms for certain periods, each period is divided examines the data stored in the database. In this phase of the working fluid distributed over the same time (T1, T2, ..., Tn), the same period are approximately the elements according to the first phase (in this work, n = 8). Whenever by type (Ti) is assigned to the test. For example, if the drop rate T3 package test device. Any period (Ti) in the same period (T1, T2, ..., TM), the number m of the cluster system. (Note: at this stage, such as T in the data collection phase). This mechanism for the calculation of the average of the properties of the corresponding head value. When the self-protection system to complete all processes of data devices begin the test liquid header information flow and get the head of the first team. As shown in 5

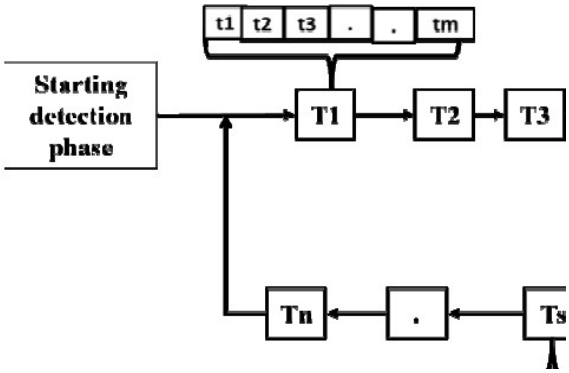

Figure 5: Split Test time with including the cluster heads & sensor nodes.

2.3. Attack

At this stage of self-defence system of the following stages: Select a message to each node in the area, message boards to control all nodes in the region to different positions depending on the type of attack.If the device detects an attack Wormhole sends the base station a message to all nodes in the area, message boards all nodes in the area to choose a different path for each shipment like alarming administrator.

2.4. Self Defence System

At this stage, the abnormal transport and protection information in advance alert the immune transport network for the attack and said data manager and the attacks of disks used in the future, when the power of the attack is attacked,

Journal of Theoretical and Applied Information Technology
15th January 2018. Vol.96. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

which causes this abnormal behaviour. Evaluate the use of the device[26,27]:

• Analysis Report: The release rate (DR) is the percentage of time that an attack is calculated noticed, when the adjustment stop their similar time in Equation 1:

$$DR_i = \sum_{i=1}^{n} \frac{N_{i,j}}{\quad} \quad \text{-----} \quad \text{Eqn:1}$$

3. Simulation Result

We have the NS-2 simulator for food self [17] system. Simulation parameters are: Types of channels: wireless channel, radio-diffusion model: Distribution / Ray Two kinds of surface-to-interface PHY / PHY wireless / LAN 802_15_4 type of Mac: Mac / 802_15_4, queue type interface queue / fall back / types PriQueue LL link layer, pattern antenna, antenna / Omni antenna, a plurality of nodes CH (cluster headache): 8 heads, a base station node station, the base station, the number of sensor elements, sensor nodes 80. in this will ever weather simulation with the emotions of many kinds of collision attacks impact (attack a brute force attack, wormholes attack run, hello fall Flood Sybil attack, sinkholes attack, stroke, and selective removal. [18] L 'we did, to identify the simulation results for intrusion detection to level. 6 [28-36].

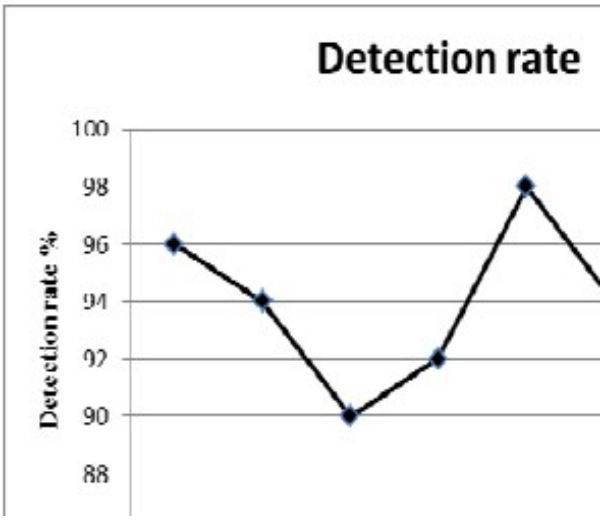

Figure 6: Detection Rate W.R.T. Attack Type

The results showed that the visual layout lower price and an average of more than 90% of all kinds of attacks work. The figures 7, 8 and 9 show the effect of the attacks on the publication of the case Halo flooding, sinkholes and worm attacks[37-40].

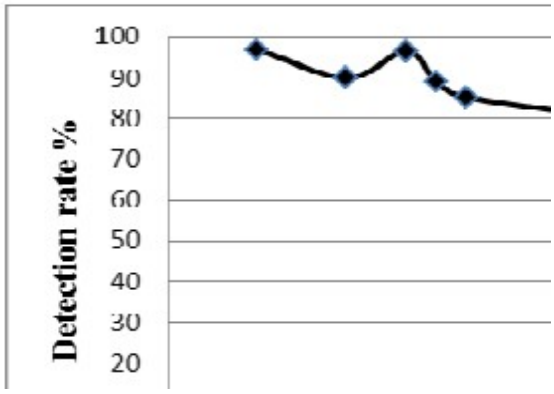

Figure 7: Effect of Number Of Hello Flood Attack On Detection Rate

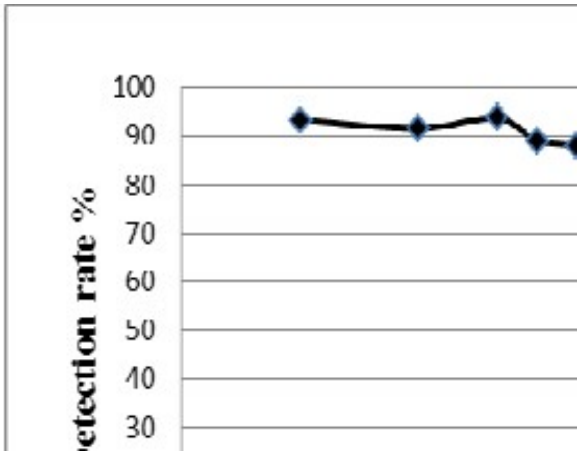

Figure 8: Effect of Number Of Wormhole Attack On Detection Rate

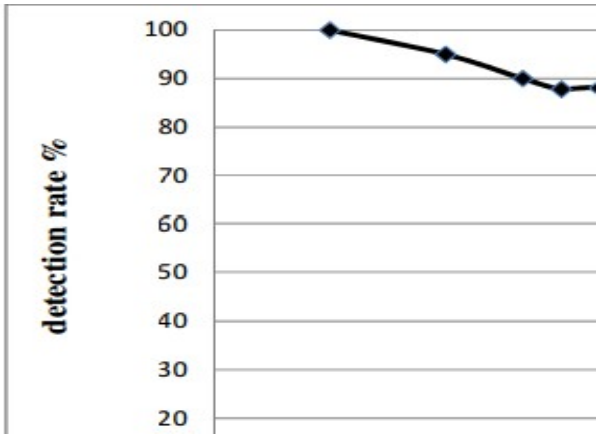

Figure 9: Number of Sinkhole Attack On Detection Rate

As shown in Figures (7, 8, and 9), to increase the number of attacks effect on the detection level,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

but, as indicated, the exposure level is 90%, which demonstrates the effectiveness of the device. Photos 10, 11 and 12 to show the impact of the attacks revelations. If Hello assault flooding, subsidence and worms[41-42ss].

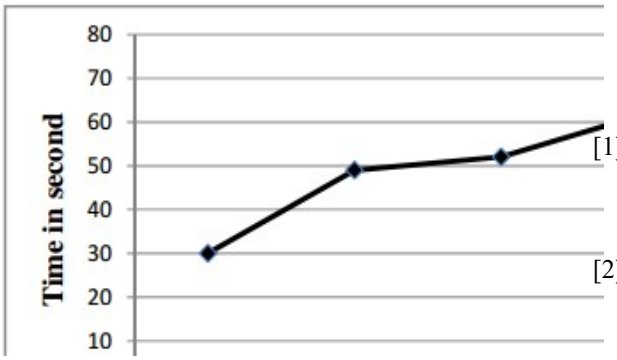

Figure 10: Time Token to Detect Wormhole Attack

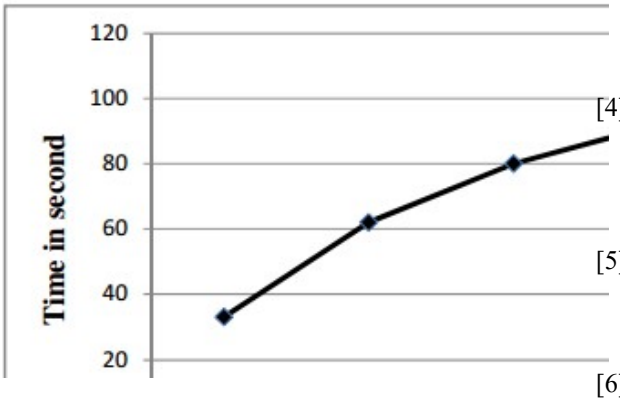

Figure 11: Time Token to Detect Wormhole Attack

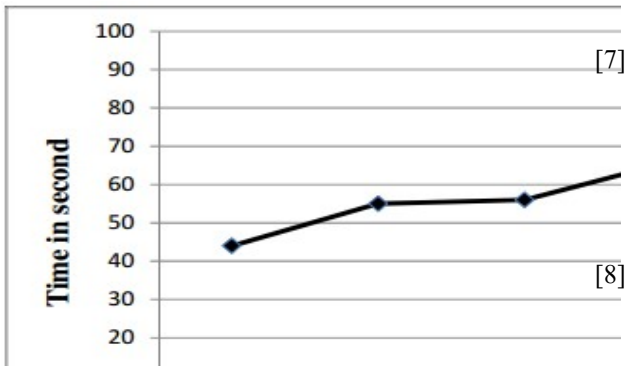

Figure 12: Time Token to Detect Sinkhole Attack

The number of attacks to influence on the detection, but as shown, the intervention shorter than 90 seconds and shows the performance of the material

4. CONCLUSION

This article outlines external aggressions protect WSN tool. This device can be of different types of attacks that are not known, and to give the unknown. The results showed that the system works best. future research is to build a test and concrete results.

REFERENCES:

[1] C. Karlof and D. Wagner: Secure Routing in Wireless Sensor networks: Attacks And Countermeasures, Ad Hoc Networks, vol. 1, pp. 293-315, 2003.

[2] Saurabh Singh Dr. Harsh Kumar Verma, "Security For Wireless Sensor Network", International Journal on Computer Science and Engineering (IJCSE).

[3] L. Alazzawi and A. Elkateeb, "Performance Evaluation of the WSN Routing Protocols Scalability", Journal of Computer Systems, Networks, and Communications, 2008, Pp1-10.

[4] A nserGhazzaal Ali Alquraishee and JayaprakashKar, "A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks", Contemporary Engineering Sciences, 2014, 135 – 147.

[5] Yao-Tung Tsou, Chun-Shien Lu, Member, IEEE, and Sy-Yen Kuo, "MoteSec-Aware: A Practical Secure Mechanism for Wireless Sensor Networks", IEEE, 2013, 2817-2829

[6] X. Du, Y. Xiao, M. Guizani, and H. H. Chen, "An effective key management scheme for heterogeneous sensor networks," Ad Hoc Networks, vol. 5, no. 1, pp. 24–34, 2007.

[7] Yi-an Huang , Wei Fan , Wenke Lee , Philip S. Yu: Cross-feature analysis for Detecting Ad-Hoc Routing Anomalies, Proceedings of the 23rd International Conference on Distributed Computing Systems, p.478, May 19-22, 2003. ZhihuaHu,BochunLi,"Fundamental Performance Limits of Wireless Sensor Networks".

[8] Gaurav Sharma, SumanBala, A K Verma and Tej Singh.Article:"Security in Wireless Sensor Networks using Frequency Hopping." International Journal of Computer Applications 12(6):15, December 2010.

[9] Dorothy E. Denning,An intrusion detection model.IEEEransactions on Software Engineering.1987. [11] Youcai Zhou, Tinglei Huang, A Statistic Anomaly Intrusion Detection Method For WSN, Microcomputer information ,2009(in chinese).

[10] Libin Yang, Dejun Mu, XiaoyanCai, An Anomaly Detection Scheme for Wireless Sensor Networks

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Based on Kernel Clustering•, Chinese Journal of Sensors and Actuators•C2008.8(in chinese) .

[11] Wang Huaibin,YuanZhang.Intrusion Detection for Wireless Sensor Networks Based on Multi-agent and Refined Clustering[C].Communications and Mobile Computing•C2009.

[12] Qi Zhu Rushun Song, YongxianYao,SVM-based cooperation intrusion detection system for WSN,Application Research of Computers,2010.4(in chinese).

[13] Yang Liu,YuFengqi,Immunity-based intrusion detection for wireless sensor networks,IEEE World Congress on Computational Intelligence•C2008.

[14] SarjounS.Doumit, Dharma P. Agrawal, Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks, MILCoM :IEEE Military Communications Conference.2003.

[15] K. Fall and K. Varadhan, "The ns manual", User's manual, UC Berkeley, LBL, USC/ISI, and Xerox PARC, January 2009.

[16] Mohammad Sadeghi, FarshadKhosravi, KayvanAtefi, Mehdi Barati, "Security Analysis of Routing Protocols in Wireless Sensor Networks", IJCSI, 2012, 456-472.

[17] J. Hubaux, L. Buttyan, and S. Capkun, "The quest for security in mobile ad hoc networks," in Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC 2001), 2001.

[18] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing robust and ubiquitous security support for mobile ad-hoc networks," in ICNP, 2001, pp. 251–260.

[19] Manel Guerrero Zapata, "Secure ad-hoc on demand distance vector (SAODV) routing," IETF MANET Mailing List, Message-ID: 3BC17B40.BBF52E09@nokia.com, Available at ftp://manet.itd.nrl.navy.mil/pub/manet/2001-10.mail, October 8, 2001.

[20] Haiyun Luo, Petros Zefros, Jiejun Kong, Songwu Lu, and Lixia Zhang, "Self-securing ad hoc wireless networks," in Seventh IEEE Symposium on Computers and Communications (ISCC '02), 2002.

[21] Jim Binkley and William Trost, "Authenticated ad hoc routing at the link layer for mobile systems," Wireless Networks, vol. 7, no. 2, pp. 139– 145, 2001.

[22] Bridget Dahill, Brian Neil Levine, Elizabeth Royer, and Clay Shields, "A secure routing protocol for ad-hoc networks," Tech. Rep. UM-CS2001-037, Electrical Engineering and Computer Science, University of Michigan, August 2001.

[23] Jiejun Kong, Haiyun Luo, Kaixin Xu, Daniel Lihui Gu, Mario Gerla, and Songwu Lu, "Adaptive security for multi-layer ad-hoc networks," Special Issue of Wireless Communications and Mobile Computing, Wiley Interscience Press, 2002.

[24] N. Modadugu, D. Boneh, and M. Kim, "Generating RSA keys on a handheld using an untrusted server," in RSA 2000, 2000.

[25] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002), June 2002, pp. 3–13.

[26] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," Tech. Rep. TR01-383, Department of Computer Science, Rice University, December 2001.

[27] Stefano Basagni, Kris Herrin, Emilia Rosti, and Danilo Bruschi, "Secure pebblenets," in ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc 2001), October 2001, pp. 156–163.

[28] A. D. Wood and J. A. Stankovic(2002) "Denial of service in sensor networks", Computer, 35(10):54–62, 2002.

[29] A. Perrig, R. Szewczyk, V. Wen et al.,"SPIN:security protocols for sensor network," Wireless Network,Vol.8.,No.5,pp. 521-534,2002.

[30] A. K. Pathan, H. W. Lee, and C. S. Hong, " Security in wireless sensor network: issues and challenges," In proceeding of the 8th ICACT 06,Volume 2, Phoenix Park, Korea, pp. 1043-1048,February, 2006

[31] Chris Karlof, Naveen Sastry, David Wagner, (2004)Tiny Seca link layer security architecture for wireless sensor networks, Proceedings of the 2nd international conference on Embedded networked sensor systems

[32] Al-Sakib khan Pathan et.al,(2006) "Security in wireless sensor networks: Issues and challenges" in feb.20-22,2006,ICACT2006,ISBN 89-5519-129-4 pp(1043-1048)

[33] Abhishek Panday, R. C. Tripathi, "A Survey on Wireless Sensor Network Security" International Journal of Computer Application(0975-8887) Volume 3- No.2, June 2010

[34] Adrian Perrig, John Stankovic, and David Wagner, (2004) "Security in wireless sensor networks" Commun.ACM,47(6):53-57.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[35] Jinat Rehana, "Security of Wireless Sensor Network" TKK T-110.5190 Seminar on Internetworking, April 2009

[36] A. D. Wood and J. A. Stankovic,(2002) "Denial of service in sensor networks", Computer, 35(10):54–62, 2002.

[37] Kalpana Sharma, M K Ghose "Wireless Sensor Network: An Overview on its Security" IJCA Special Issue on "Mobile Ad-hocNetwork" MANETs 2010

[38] Mayank Saraogi . Security in Wireless Sensor Networks. In ACM SenSys, 2004.

[39] S. Datema. A Case Study of Wireless Sensor Network Attacks. Master's thesis, Delft University of Technology, September 2005.

[40] Sophia Kaplantzis, "Security Models for Wireless Sensor Networks" March 20, 2006

[41] C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems, pages 162–175, New York, NY, USA, 2004. ACM Press.

[42] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen, "SPINS: Security Protocols for Sensor Networks", Department of Electrical Engineering and Computer Sciences, University of California, Berkley, 2002.