COLLATION OF SECURITY FOR ASSORTED ATTACKS IN WIRELESS SENSOR NETWORKS

R.M.Dilip Charaan[1], Dr.R.Ramesh[2]

[1]*Research Scholar, Department of Computer Science and Engineering,*
College of Engineering Guindy,Anna University, Chennai,(India)
[2]*Associate Professor, Department of Electrical and Electronics Engineering,*
College of Engineering Guindy,Anna University, Chennai,(India)

ABSTRACT

The rise of wireless sensor networks (WSN) as one of the predominant innovation slants in the nearing decades has postured various one of a kind difficulties to scientists. The sensing innovation joined with handling force and wireless correspondence makes it lucrative for being misused in future. The incorporation of wireless correspondence innovation too brings about different sorts of security dangers. The aim of this paper is to explore the security related issues, the difficulties and to propose some answers for secure the WSN against these security dangers. While the set of difficulties in sensor systems are assorted, this paper concentrate just on the difficulties identified with the security of sensor networks. This paper likewise also proposes a percentage of the security objective for Wireless Sensor Networks (WSN).

Keywords: Attacks, Defense, Security, Wireless Sensor Networks,

I. INTRODUCTION

For any Wireless Sensor Networks (WSNs) to gather data from the physical world is the main objective. Advances in wireless correspondence made it conceivable to create wireless sensor networks (WSN). Presently a day's wireless sensor systems (WSNs) have been distinguished as one of the rising innovations. A WSN comprise of spatially circulated independent sensor hubs to helpfully screen physical or natural conditions. The hubs convey in wireless design. Source hubs transmit their information to destination hub either specifically or through middle hubs. These destination hubs are joined with a focal portal, otherwise called base station or sink node. Base station gives association with wired world where information can be gathered, prepared and broke down. These sensor hubs are utilized for occasion discovery and consistent sensing which comprise of handling unit (for information handling), Sensing unit, battery (for vitality).Contrasting with existing systems, wireless sensor networks can essentially work in any environment. WSNs are frequently sent to sense, transform and disperse data of focused on physical situations. As a rule, WSNs comprise of battery-worked sensor gadgets with registering, information handling, and conveying parts. The ways the sensors are conveyed can either be in a controlled situation where checking and observation are discriminating or in an uncontrolled situation.

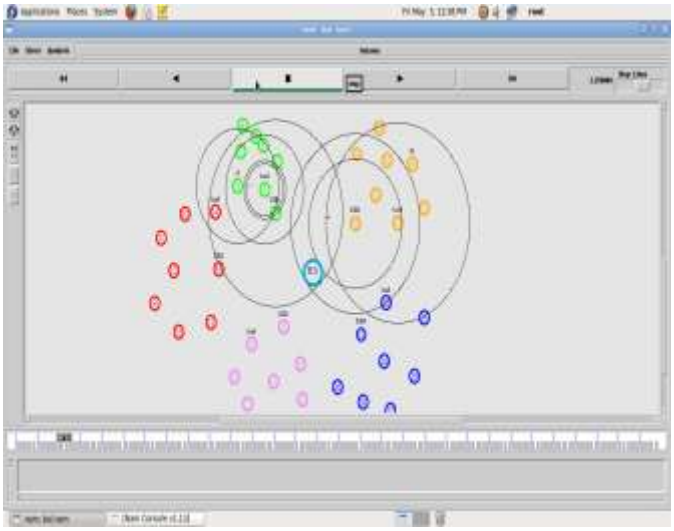
In the uncontrolled situations, security for sensor systems gets to be to a great degree essential. Its expense relies on upon its parameters like memory size, transforming velocity and battery [4]. As these sensor hubs are of minimal effort, a system of hundreds or a huge number of hubs are likewise conceivable which serves to

upgrade the scope zone and also unwavering quality of system. These sensors have information handling and correspondence capacities [23]. They sense the conditions in which they are encompassed and change their information to electronic signs. The electronic signs are transmitted over radio waves to the base station (BS). It is wasteful for all the sensors to send their information straightforwardly to the BS as sensor hubs are vitality compelled. Since information produced from neighboring sensors is excess, the measure of information created in expansive systems is normally gigantic for the BS to process. To take care of these issues, we can perform information collection in sensor hubs.

Data aggregation includes the combination of information from various sensor hubs at moderate hubs and transmission of collected information to the BS or Sink. Information accumulation can dispense with excess; minimize the quantity of transmissions and subsequently spare vitality. The utilization of wireless sensor systems is expanding step by step and in the meantime it confronts the issue of vitality limitations regarding constrained battery lifetime. As every hub relies on upon vitality for its exercises, it is important to enhance system lifetime of wireless sensor organizes by adequately diminishing vitality utilization. To accomplish this objective numerous directing calculations have been proposed. Among all the proposed strategies, progressive steering conventions extraordinarily fulfill the restrictions and imperatives in WSNs[1]. It is essentially considered as a two layer structural engineering where one layer is occupied with bunch head determination and the other layer is in charge of steering. A cluster head (CH) in progressive steering is the hub which is in charge of gathering information from different hubs in the group, amassing all information and sending the collected information to the base station.

WSNs are susceptible to different attacks especially physical attacks these are the most malicious and harmful attacks. Due to the unsafe defenceless nature of the communication channel, untrustworthy transmission media and limited resources many security techniques are not possible. Hence for the conventional networks, security is a vital requirement to put away from a range of attacks. The objective is to design an appropriate security mechanism for these networks that must be designed considering the various security dimensions of WSN's included confidentiality, integrity, availability and authenticity.

This is a wireless sensor network with five clusters where the data is being transmitted from one node and another node using LEACH (Low Energy Adaptive Clustering Hierarchy) protocol.



II.ISSUES IN SECURITY FOR WSN

Security mechanisms in WSN are developed from considering certain constraints. There are few pre-defined security strategies; some are direct consequences of the hardware limitations of sensor nodes.

2.1 Energy Efficiency: The requirements for energy efficiency offer an idea that computation is favored over communication. This is because communication has three orders of magnitude which is more expensive than computation [10]. Security should never be overdone also tolerance is preferred to overaggressive prevention. Using computational power intensive algorithms should not be used to incorporate security as energy is considered [17].

2.2 No public key cryptography: Public key cryptographic algorithms are expensive on sensor nodes both in terms of storage and energy [8]. Security schemes should never rely on public key cryptography and this is more reliable for smaller networks [10].

2.3 Physical tampering: Sensor nodes are low cost hardware and are not built with tamper resistance, their strength in the number [7][9]. Even though few nodes go down, the network thrives. The network should be resilient to attacks [10].

2.4 Multi layers of defense: Security turns into a vital concern in light of the fact that attacks can happen on diverse layers of a systems administration stack[7]. Naturally it is apparent that a different layer of barrier is required i.e. a different resistance for every layer. The issues specified here are all in all pertinent to pretty much a wide range of area independent of their attributes.

III.VARIOUS SECURITY DIMENSIONS

3.1 Availability

Sensors are emphatically compelled by numerous elements, e.g., constrained reckoning and correspondence capacities. Extra interchanges expend extra vitality and if there is no more vitality, information won't be accessible. Vitality is an alternate to a great degree constrained asset in expansive scale remote sensor systems. A solitary point disappointment will be presented while utilizing the essential issue plan. This extraordinarily debilitates the accessibility of the system. The prerequisite of security not just influences the operation of the system, additionally is exceedingly imperative in looking after the accessibility of the entire system. Besides, remote sensor systems are defenseless to different attacks[18]. The foe is expected to have more assets, for example, compelling processors and lavish radio transmission capacity than sensors. Outfitted with wealthier assets, the foe can dispatch significantly more genuine attacks, for example, DOS attack, asset utilization attack and hub bargain attack.

3.2 Confidentiality

Information confidentiality is the most essential issue in system security. Confidentiality, integrity and authentication security administrations are obliged to defeat the attacks from enemies specified in the above area. These security administrations are attained to by cryptographic primitives as the building pieces.[18]

Confidentiality implies that unapproved outsiders cannot read data between two conveying gatherings. A sensor system ought not spill sensor readings to its neighbors.

Particularly in a military application, the information put away in the sensor hub may be very delicate.

• In numerous applications, hubs convey exceedingly touchy information, e.g., key distribution; in this way it is to a great degree critical to construct a protected direct in a remote sensor system.

• Public sensor data, for example, sensor characters and open keys, ought to additionally be scrambled to some degree to ensure against traffic analysis attacks. For the most part, encryption is the most broadly utilized system to deliver confidential messages.

3.3 Classifiedness

This implies that unapproved outsiders cannot read data between two conveying gatherings. A sensor system ought not to spill sensor readings to its neighbors. Particularly in a military application, the information put away in the sensor hub may be profoundly touchy. In numerous applications, hubs impart profoundly delicate information, e.g., key circulation; thus it is amazingly imperative to manufacture a safe divert in a remote sensor system [18]. Open sensor data, for example, sensor personalities and open keys, ought to likewise be scrambled to some degree to secure against movement investigation attacks. For the most part, encryption is the most generally utilized instrument to give secrecy.

3.4 Integrity and Authenticity

Secrecy just guarantees that information cannot be perused by the outsider, yet it doesn't promise that information is unaltered or unaltered. Uprightness implies the message one gets is precisely what was sent and it was unaltered by unapproved outsiders or harmed amid transmission. Remote sensor systems are more helpless against eavesdropping and message modification [6]. Measures for ensuring trustworthiness are expected to recognize message adjustment and to reject infused message. Authentication guarantees that the sender was qualified for make the message and that the substance of the message has not been adjusted. In people in general key cryptography, computerized marks are utilized to seal a message as a method for authentication. In the symmetric key cryptography, MACs are utilized to give authentication. At the point when the collector gets a message with a confirmed MAC, it is guaranteed that the message is from a unique sender. Computerized mark is in view of asymmetric key cryptography (e.g., RSA), which includes significantly more processing overhead in marking/unscrambling and confirming/scrambling operations. It is less strong against DOS attacks subsequent to an aggressor may encourage an exploited person hub with countless fake marks to fumes the exploited person's calculation assets for confirming them.

3.5 Data Freshness

Data freshness implies that the information is late and any old information has not been replayed. Information freshness criteria are an unquestionable requirement in the event of imparted key cryptography where the key needs to be invigorated more than a time of time. An aggressor may replay an old message to trade off the key. Security attacks in sensor systems can be comprehensively ordered into Passive attacks and Dynamic attacks. Passive attacks are in the way of eavesdropping on, or observing of, transmissions [22]. The thought process of the aggressor is to acquire data that is being transmitted. Two sorts of passive attacks are arrival of message substance and movement investigation. Dynamic attacks include some alteration of the information stream or

the formation of a false stream and can be subdivided into four classifications: masquerade, replay, alteration of messages, and disavowal of administration. Fundamentally we are predominantly looking .at two sorts of security: assurance from dissent of-administration (DOS) attacks, and insurance of the mystery of data. Various barriers, each for one layer of the systems administration stack ought to be actualized. One layer is examined at once: The Physical layer alludes to mechanical, electrical, useful and procedural qualities to build, keep up and discharge physical associations (e.g. information circuits, radio interfaces) between information join substances. This layer characterizes certain physical qualities of the system, for instance the recurrence, the information rate, the sign tweak and the spread range plan to utilize.

IV. TYPES OF ATTACKS ON WSN

Since the nodes of a wireless sensor networks are placed in the hostile environment they are vulnerable to attacks.

Attacks on WSNs are classified are of two different levels

1. Attack against security mechanisms.
2. Attack against basic mechanisms.(e.g. routing)

In many cases, the information gathered by the sensing nodes has to be maintained confidential and it should be authentic [11]. In the non-attendance of security a malicious node could interrupt undisclosed information, or possibly will send fake messages in the network. The major attacks are: Sybil attack, Selective Forwarding attack, Denial of Service (DOS), Wormhole attack, Sinkhole attack, Passive information gathering, Node capturing, malicious node, Hello flood attack etc.

4.1 DOS Attack

It happens by the inadvertent disappointment of hubs or malevolent activity. The least complex DOS attack tries to fumes the assets accessible to the exploited person hub, by sending additional superfluous parcels and in this way keeps real system clients from getting to administrations or assets to which they are entitled[1][2]. DOS attack is implied not just for the adversary's endeavour to subvert, upset, or demolish a system, additionally for any occasion that reduces a network's ability to give an administration [2]. In remote sensor arranges, a few sorts of DOS attacks in distinctive layers may be performed. At physical layer the DOS attacks could be sticking and altering, at link layer, crash, weariness, shamefulness, at system layer, disregard and greed, homing, confusion, dark gaps and at transport layer this attack could be performed by malevolent flooding and desynchronization.

4.2 Wormhole Attack

One hub in the system (sender) makes an impression on the an alternate hub in the system (beneficiary node)[11].Then the getting hub endeavours to send the message to its neighbours. The neighbouring hubs think the message was sent from the sender node (which is for the most part out of extent), so they endeavour to send the message to the beginning hub; however it never lands since it is too far away.

Wormhole attack is a huge risk to remote sensor systems, on the grounds that, this kind of attack does not require bargaining a sensor in the system rather, it could be performed even at the introductory stage when the sensors begin to find neighbouring data [13]. Wormhole attacks are hard to counter in light of the fact that steering data supplied by a hub is hard to check.

4.3 Sybil Attack

In this attack, a solitary hub i.e. a vindictive hub will seem to be a set of hubs and will send off base data to a hub in the system. The off base data can be an assortment of things [11], counting position of hubs, sign qualities, making up hubs that don't exist. Confirmation and encryption systems can keep a pariah to dispatch a Sybil attack on the sensor system. In any case, an insider can't be kept from taking an interest in the system; be that as it may he ought to just have the capacity to do as such utilizing the personalities of the hubs he has traded off. Open key cryptography can anticipate such an insider attack, however it is so lavish it couldn't be possible be utilized as a part of the asset compelled sensor systems.

4.4 Node Capturing Attack

A specific node may be selected in random and that particular node might be captured and the date might be collected by the malicious node.

4.5 Sinkhole Attack

In a sinkhole attack, the adversary's point is to bait almost all the activity from a specific territory through a traded off hub, making an allegorical sinkhole with the foe at the focal point [4]. Sinkhole attacks normally work by making a bargained hub look particularly appealing to encompassing hubs with deference to the directing calculation. Sinkhole attacks are hard to counter on the grounds that steering data supplied by a hub is hard to confirm. As a case, a laptop-class foe has an in number force radio transmitter that permits it to give a top notch course by transmitting with enough power to achieve a wide region of the system [3].

V. DEFENSIVE MECHANISM

5.1 DOS Attack Prevention

The instruments to avert DOS attacks incorporate instalment for system assets, pushback, solid confirmation and distinguishing proof of movement [1] [2]. One security strategy employments confirmation streams to secure the reinventing methodology. These partitions a system paired into a progression of messages, each of which contains a hash of the following message. This instrument guarantees that an interloper can't capture a progressing project transmission, regardless of the possibility that he or she knows the hashing system. This is on the grounds that it would be practically difficult to develop a message that matches the hash contained in the past message. A digitally marked notice, which contains the system name, variant number, and hash of the first message, guarantees that the procedure is safely launched [2]. We can vanquish numerous dangers utilizing existing encryption and validation systems, and different methods, (for example, distinguishing sticking attacks) can ready system chairmen of continuous attacks or trigger strategies to save vitality on influenced gadgets [1].

5.2 Wormhole Attack Prevention

The instrument to battle the wormhole attack incorporate, DAWWSEN [14] , a proactive directing convention based on the development of a various levelled tree where the base station is the root hub, and the sensor hubs are the inner or the leaf hubs of the tree. An incredible point of interest of DAWWSEN is that it doesn't require any topographical data about the sensor hubs, and doesn't take the time stamp of the packet as a methodology for recognizing a wormhole attack, which is essential for the asset obliged nature of the sensor.

5.3 Sybil Attack Prevention

The systems to avoid against Sybil attacks are to use character certificates [12]. The essential thought is extremely basic. The setup server, before organization, doles out every sensor hub some exceptional data. The server then makes a character declaration tying this node's character to the doled out exceptional data, furthermore downloads this data into the hub. To safely exhibit its personality, a hub first displays its character authentication, and afterward demonstrates that it has or matches the related exceptional data. This procedure requires the trade of a few messages Merkle hash tree can be utilized as fundamental method for figuring character certificates.

The Merkle hash tree is a vertex-marked parallel tree, where the mark of each non-leaf vertex is a hash of the linking of the names of its two tyke vertexes. The essential way of a leaf vertex is the situated of vertexes on the way from the leaf to the foundation of the tree. The validation way comprises of the kin of the vertexes on this essential way. Given a vertex, its verification way, and the hash work, the essential way can then be registered, up to and counting the base of the tree. This figured estimation of the root can then be contrasted and a put away esteem, to confirm the genuineness of the mark of the leaf vertex [12].

5.4 Node Capture Attack Prevention

On the off chance that a hub has been bargained then how to reject that hub furthermore that hub just, from the sensor system is at issue. This issue is illuminated by (LEAP). Jump (confined encryption and confirmation convention) is a proficient convention for between hub movement validations. This convention depends on a key imparting methodology that approves in-system transforming, and in the meantime mitigates various conceivable attacks.

5.5 Sinkhole Attacks Prevention

Such attacks are extremely hard to safeguard against. One class of conventions impervious to these attacks is geographic steering conventions. Geographic conventions develop a topology on interest utilizing just restricted associations and data and without launch from the base station [16].

5.6 Selective Forwarding Attacks

Multipath routing can be utilized to counter these sorts of selective forwarding attacks. Messages directed over ways whose hubs are totally disjoint are totally secured against selective forwarding attacks including at most traded off Allowing hubs to powerfully pick a packet's next jump probabilistically from a set of conceivable hopefuls can further lessen the shots of an enemy increasing complete control of an information[17].

VI. PHYSICAL ATTACKS AND ITS EFFECTS ON WIRELESS SENSOR NETWORKS

WSN's are designed as a layered architecture which makes these kinds of networks susceptible. This acts as a wall against many kinds of attacks [23]. The following table presents the details regarding the physical attacks.

Table 1 Physical Attacks And Its Effects

Attacks	Description	Techniques	Effects
Signal/Jamming	This tries to transfer radio signals emitted	Deceptive jamming, reactive jamming,	Radio meddling ,resource fatigue

		random jamming	
DOS(Path-Based)	Combinations of attacks include jamming attacks	To the base station huge packets of data are sent.	Accumulator in the nodes get exhausted, network disruption reducing WSNs availability.
Eavesdropping	By overhearing the contents of the communication	Misusing the wireless character of the sensor networks transmission medium, interception	inducting few other assaults, extracting sensitive WSN data, Deleting privacy protection,
Node capturing attack, Device tampering attack	Direct physical access, captive and replaced nodes	Eavesdropping, Invasive attacks, non-invasive attacks,	smash up or transform physically alter node's services,
DOS attacks	Attacks in different layers of WSN's this reduces WSN,s availability.	Physical layer, Network layer, transport layer, application layer.	Effects of all the layer attacks(Physical layer, Network layer, transport layer, application layer)[14]

The table shows the various types of attacks in each layer, attack type, security mode and its best choice which might be given to the nodes in the wireless sensor nodes in order to control the attacks to a larger extent[23][3].

Table 2 Different Types Of Attack

Layer	**Attack Type**	**Security mode**	**Optimal choice**
Physical Layer	DOS attacks	DSSS/FHSS	FHSS around 1000 hops/second using Frequency Shift Keying
	Physical tampering		Use a hardware that is tamper resistant
Application layer	Assaults based on Aggregation		Aggregation
Data link layer	Jamming of data packets	Encryption	programme switching
Network Layer	Sybil	Pre-distribution of random keys,	Key management Architecture
	Black holes	Schemes based on Key Management	REWARD algorithm[19]
	Wormholes	TIK[20]	Symmetric cryptography

VII. CONCLUSION

WSN security is a critical issue which is persuaded towards guaranteeing security under the strict requirements of computational force, vitality and other equipments. Besides, the accompanying focuses can be included. Security of a WSN is subject to securing for all the layers. From multiple points of view security has been seen as a standalone part of a framework's construction modeling or idea in retrospect, where a different module gives security. To attain a protected framework, security must be embedded into each part. As a rule not coordinating security to parts amid framework advancement outline, part has turned to be a state of assaults. The proposed methodology addresses a few viewpoints, being exceptionally adaptable and ready to be effectively adjusted to various types of situations when contrasted and the accessible methodologies. However a coordinated methodology of secured steering convention and key-administration construction modeling would without a doubt yield a superior security measure for the Wireless Sensor Networks.

REFERENCES

[1] A.D. Wood and J.A. Stankovic, (2002) “Denial of Service in sensor networks”, Computer, vol. 35, no. 10, 2002, pp. 54– 62.

[2] David R. Raymond and Scott F. Midkiff,(2008) "Denial-of- Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, 2008, pp. 74-81.

[3] E. C. H. Ngai, J. Liu, and M. R. Lyu, (2006)“On the networks,” in Proceedings of the IEEE International Conference on Communications (ICC ‟06), Istanbul,Turkey.

[4] Kalpana Sharma”Wireless Sensor Networks: An Overview on its Security Threats ”,IJCA Special Issue on “Mobile Ad-hoc Networks”,MANETs, 2010 ,pp 42-45.

[5] Dr. G. Padmavathi, et al “ A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks “ (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009 .pp 1-9

[6] Adrian Perrig, John Stankovic, and David Wagner. Security in wireless sensor networks. Commun.ACM, 47(6):53.57, 2004.

[7] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: challenges and solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47, Feb. 2004.

[8] D. Carman, B. Matt, D. Balenson, and P. Kruus, "A communications security architecture and cryptographic mechanisms for distributed sensor networks," in DARPA SensIT Workshop. NAI Labs, The Security Research Division Network Associates, Inc., 1999.[Online]. Available: http://download.nai.com/products/media/pgp/pdf/sensit-workshop- 100799.pdf

[9] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of the 2003 IEEE Symposium on Security and Privacy. IEEE Computer Society, 2003.

[10] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in Third IEEE International Conference on Pervasive Computing and Communications (PERCOM'05). IEEE Computer Society Press, 2005, pp. 324-328.

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

[12] J. R. Douceur,(2002) "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS "02).

[13] Zaw Tun and Aung Htein Maw,(2008)," Worm hole Attack Detection in Wireless Sensor networks", proceedings of world Academy of Science, Engineering and Technology Volume 36, December 2008, ISSN 2070-3740.

[14] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, (2005)" DAWWSEN: A Defense Mechanism against Wormhole ttack In Wireless Sensor Network",Proceedings of the Second International Conference on Innovations in Information Technology (IIT"05).

[15] George S.Oreku"Reliability in WSN for security: Mathematical Approach",IEEE, 2013

[16] M. Zorzi and R. R. Rao, (2003) "Geographic Random Forwarding (GeRaF) for Ad Hoc and Sensor Networks: Transactions on Mobile Service in Wireless Sensor Networks: Attacks and Computing, vol. 2, no. 4, pp. 337-348, 2003.

[17] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks,"Mobile Computing and Communications Review, vol. 4, no. 5, October 2001.

[18] Security in Distributed, Grid, and Pervasive Computing Yang Xiao,(Eds.) pp. 2006 Auerbach Publications, CRC Press Wireless Sensor Networks: An Overview on its Security Threats.

[19] Karakehayov, Z., "Using REWARD to detect team black-hole attacks in wireless sensor networks", in Workshop on Real-World Wireless Sensor Networks (REALWSN'05), 20-21 June, 2005, Stockholm, Sweden.

[20] Hu, Y.-C., Perrig, A., and Johnson, D.B., "Packet leashes: a defense against wormhole attacks in wireless networks", Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies.IEEE INFOCOM 2003, Vol. 3, 30 March-3 April 2003, pp. 1976 – 1986

[21] F. Stajano and R. Anderson. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In Proceedings of The 7th International Workshop on Security Protocols, volume 1796 of LNCS, pages 172–194. Springer- Verlag, 2000.

[22] Ian F. Akykildiz, Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci, "A Survey on Sensor Networks", IEEE Communication Magazine, year 2002

[23]Rina Bhattacharya "A Comparative Study Of Physical Attacks On Wireless Sensor Networks"IJRET: International Journal of Research in Engineering and Technology,Volume: 02 Issue: 01,Jan-2013 pp 72-74.

[24] Kalpana Sharma et al "A Comparative Study of Various Security Approaches Used in Wireless Sensor Networks", International Journal of Advanced Science and Technology , Vol. 17, April, 2010, pp 42-45