International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:5, No:8, 2011

Challenges for Security in Wireless sensor Networks (WSNs)

Muazzam A. Khan, Ghalib A. Shah, Muhammad Sher

Abstract**—**Wireless sensor network is formed with the combination of sensor nodes and sink nodes. Recently Wireless sensor network has attracted attention of the research community. The main application of wireless sensor network is security from different attacks both for mass public and military. However securing these networks, by itself is a critical issue due to many constraints like limited energy, computational power and lower memory. Researchers working in this area have proposed a number of security techniques for this purpose. Still, more work needs to be done.In this paper we provide a detailed discussion on security in wireless sensor networks. This paper will help to identify different obstacles and requirements for security of wireless sensor networks as well as highlight weaknesses of existing techniques.

Keywords**—**Wireless senor networks (WSNs), Security, denial of service, black hole, cryptography, stenography

I. Introduction

WIRELESS Sensor Networks (WSNs) are rapidly gaining interests of researchers from academia, industry and defense. WSNs consist of a large number of sensor nodes and a few sink nodes deployed in the field to gather information about the state of physical world and transmit it to interested users, typically used in applications, such as, habitat monitoring, military surveillance, environment sensing and health monitoring. Sensor nodes have limited resources in term of processing power, battery power, and data storage. Nodes in WSNs are passive, which can only monitor the events of interest and thus they are unable to react in the environment. Sensor nodes use wireless interfaces for communication and have short range due to limited energy [1].The sensor nodes have capabilities of self organization; there exist a complete coordination and cooperation among these nodes, which is the most important feature of these networks. Wireless sensor networks are mostly used for real time data processing in critical military operations, environmental monitoring, safety and protection of domestic infrastructure and resources. There are certain inherit limitations of these networks like lower batter power, low memory and band width [1][2]. Figure 1 presented a simple scenario of wireless sensor networks.Due to these weaknesses traditional security techniques are not suitable and efficient for wireless sensor networks. Some researchers are also working for development of a trust model for this purpose which may increase computation capabilities and decrease energy and storage utilization [3] [4]. As compare to wire networks wireless networks are more prone to attacks. There may be many types of attacks where the attacker fully destroy any network or inject/alter data in the middle. In many scenarios like emergency operation, natural disasters or battle field monitoring we can not compromise on security because any negligence can cause a huge destruction. Therefore it is important to analyze these security attacks, security requirements and various approaches used to control these attacks [5] [6] [7].This paper evaluates different security requirements for wireless sensor networks, security attacks and proposed protocols by different researchers to control these attacks. The remainder of the paper is organized as follows. In section II we present detail discussion on security requirements for wireless senor networks. Section III describes various possible attacks in WSN. Section IV discusses different techniques for detection and prevention of various security attacks. Section V presents proposed security protocol by researchers. Section VI which is the last section of this paper have conclusion and future work.

Muazzam A. Khan is PhD Scholar in Department of Computer Science, International Islamic University Islamabad, Pakistan.
Ghalib A. Shah is with the Department of Computer Engineering, College of E & M Engineering, NUST Rawalpindi, Pakistan.
Muhammad Sher is Professor and Chairman Department of Computer Science, International Islamic University Islamabad, Pakistan.

II. Security Requirements in Wireless SENSOR NETWORKS

In this section we discuss different types of security requirements for wireless sensor networks. Any compromise on these requirements can cause a huge destruction in the network. In this section we discuss different types of security requirements for wireless sensor networks. Any compromise on these requirements can cause a huge destruction in the network.

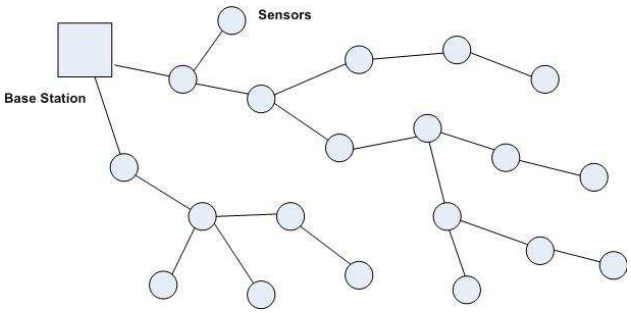

Fig. 1 Architecture of Wireless Sensor Networks

A. Data Integrity

Wireless sensor networks are mostly used for security purposes therefore data integrity is very important in such networks. Data integrity ensures that data packets received at destination is exactly the same transferred by the sender and no one in the middle alters that packet [18]. Wireless sensor networks mostly works on broadcasting therefore it is more vulnerable to such security attacks.

B. Confidentiality

Confidentiality of the network means that data transfer between sender and receiver will be totally secure and no third person can access it (neither read nor write). In military operations sensed data is very important so it may be transferred securely to achieve confidentiality and secure key distribution [19].

C. Authentication

Authentication of a sensor node ensures that he is a legitimate sensor and has the right to send data as well as the sent message by that node has the right contents. In asymmetric cryptographic communication digital signatures are used to check the authentication of any message or user while in symmetric key MAC,s are used for authentication purpose.

D. Self Organization

Sensor nodes as well as sink nodes may have flexibility to organize themselves according to changing situation especially in mobile scenarios or in case of nodes failure. In many cases some sensor nodes are failed to activate themselves or their energy may consume faster. Then the neighbour nodes may arrange themselves to control the new situation. However due to inherit problems in wireless sensor networks there are still certain issues need to be resolve.

E. Data Freshness

Data Freshness means the time when that packet was sent is recent or not. For security and avoidance of self destruction data freshness is very important in wireless sensor networks. Because an attacker can send an expire packet to waste the network resources and also cause self destruction.

F. Availability

In order to ensure the availability of network resources. The sensor nodes may survive for more time if it save its energy or properly utilize it. When there is no activity in the network or the situation is normal as accordingly then sensor nodes may go in sleep mode to save their energy and utilize it in emergency scenario. In normal situation only few nodes are in active mode of operation. Whenever there is an attack the base station is responsible to activate all sensor nodes in sleeping mode.

G. Flexibility

Wireless sensor networks play an important role in emergency scenarios and battle field. Therefore the external conditions as well as demands of the user changes rapidly. So according to the nature of mission or changing conditions the sensor nodes may have flexibility to adopt these changes.

H. Secure Localization

To locate the accurate position of the sensor node. Accurate location of a sensor node is very important for data forwarding as well as trust management. There are 2 main types of localization Range based and range free based. Range based approach is normally used in wireless sensor networks [22].

III. ATTACKS IN WIRELESS SENSOR NETWORKS

In this section we discuss different types of attacks and their affects in Wireless Sensor Networks. There are two major types of attacks in wireless sensor networks.

A. Active Attacks

These are such types of attacks in which the attacker cause destruction. There is physical damage in the network like destruction of resources, alteration of data, changing traffic direction or stoppage of data to sink nodes. These attacks are easily identifiable and we can stop the attackers as well as start the system recovery process.

B. Passive Attacks

These are another types of attacks in which the attackers only observe different activities on the network check confidential information but don't cause any physical destruction or any alteration of information. However the passive attackers can launch active attacks and cause a big damage because during observation of different activities on the network he is able to find weak points and clues in the network and wait for a suitable time to launch an attack. Passive attacks are more dangerous as compare to active attacks because in passive attacks you are unable to recognize your attacker.

C. Flood Attacks

Karlof et al [8] in 2003 introduced a flood attack in wireless sensor networks. For this purpose Hello packets are used to destroy the network resources. In this attack the attacker floods Hello messages in the network that are dispersed in the whole network. However the attacker pretended that the sender of the packet is in their neighbour, therefore when the sender node want to send any sensed information to a sink node then they forward it toward attacker node. Because they think that the attacker node is in their neighbour, and so any information forwarded toward base station in those packets can be easily accessible to attacker.

D. Black hole Attack

Culpepper et al [9] identified a new attack in wireless sensor networks that is called black hole attacks. In such type of attacks the attacker nodes act like a black hole, where the attacker node listen the route request packets from its neighbours and reply them back using fake information about shortest route toward sink node. So every node in its surrounding set the attacker as a next node for data forwarding

toward sink. Any node which wants to send data to a base station will forward it towards attacker. This provides the attacker with an opportunity to analyze these packets and extract important information. Figure 2 show a scenario of black hole attack where the attacker node receive all traffic before approaching base station and provide fake information about routes.

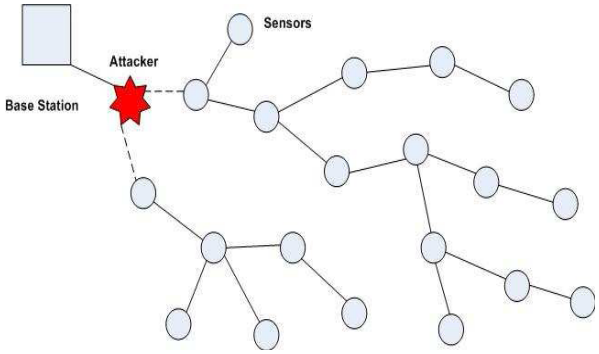

Fig. 2 Black hole Attack in Wireless Sensor Networks

E. Denial of service Attack (DoS)

Black ert et al [10] launched a new attack in wireless sensor networks. The main objective of this attack is to waste the available resources of the network. In this attack the attacker (malicious node) send extra packets in the network with out any need and keep the route as well as the base station busy. So the authentic users are unable to send data, access resources and get services. Therefore DoS attack is launched to prevent the legitimate users of the network from utilization of resources to get any service. DoS attack may vary from layer to layer in OSI model. At physical layer DoS attack may be in the form of traffic blockage and delay, at data link layer it may cause collision of frames and unfairness. DoS attack at network layer may be packet routing in wrong direction as well as black holes creation. While on transport layer DoS attack may be flooding (extra traffic) or desynchronization of data in the network [11] [12].

F. Sybil Attack

Wireless sensor networks are more vulnerable to sybil attack. In such types of attack a node changes its ID continuously and attacker nodes using multiple identities of the legitimate sensor nodes at the same time. Main purpose of this attack is to increase the resource utilization and decrease data integrity. Sybil attacks mostly happened in distributed systems on network servers for data aggregation. Although detection of such nodes that launches Sybil attacks is a very hard task. Dovcevr et al [13] proved that Sybil attacks can be controlled however in the absence of centralized controller there are more chances of Sybil attack. Therefore in wireless sensor networks we have a centralized base station which helps in prevention of Sybil attacks. Many others like Newsome et al [14] detect Sybil nodes in the network with the help of radio resources and also calculate the probability of a Sybil node in the network.

G. Information Alteration

Sensor nodes have responsibility to sense an event from its physical world and transfer that information toward a base station [15]. However in the middle of communication there is chance of spoofing data by an attacker, so he may alter the complete message or a part of it to misguide the base station. In this attack the attacker can observe all the traffic inside the network that's why if the attacker node did any alteration, we can identify it and detect the attack. However if he is only observing all the activities and ask someone else to attack then it is very difficult to detect such attackers.

H. Worm holes

In this attack the whole traffic of the network is tunnelled in a particular direction at a distant place, which causes deprivation of data receiving in other parts of the network. Sometime any information which is very important and should be deliver to the base station in specific time is sended toward worm hole [16]. Figure 3 shows a scenario of wormhole attack where the attacker node creates a loop in the network and sending data back toward those sensors.

I. Looping

In this attack few nodes in the network cause the circulation of data in a particular region. This attack stops data to send to a destination node and revolve in the same region which increase network traffic as well as causes latency [16].

J. Node Replication

In this attack the attacker add a new sensor node in the network, which is using the ID of a legitimate user. This attacker node replication can cause a big destruction in network because he can attack any node or sink node by pretending himself as a legitimate user. Once the replicated node is able to access the network then there is possibility that he may get the position of a strategic node or the security keys may be exposed [17].

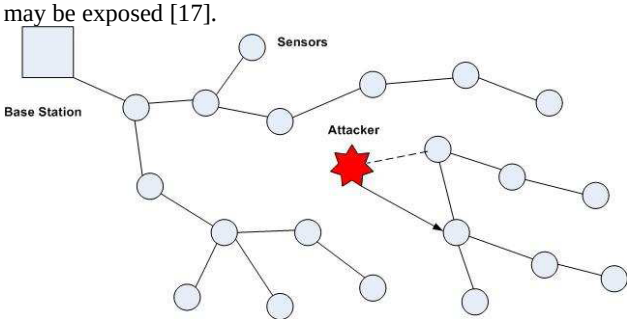

Fig. 3 Wormhole Attack in Wireless Sensor Networks

IV. Prevention And Detection Of Various Security Attacks

In this section we discuss that how to prevent and detect different security attacks in wireless sensor networks. There are many techniques with the help of which we can protect our network from different attacks like DoS attack, Spoofing, data aggregation, secure routing, intrusion detection and prevention.

A. Denial of Service Attack (DOS)

For Denial of service attack on transport layer the base station always force the sensor node to request more resources up front then the server and jamme the traffic [33]. Defending against jamming attack is to identify the jammed part of the sensor network and effectively route around the unavailable portion [34]. There are two phases in which the sensor nodes near the jammed region report their status to their directly connected neighbors, who then collaboratively define the jammed region and simply route it onward. Protection against Network IDs, as well as physical protection of whole network is necessary to prevent DoS attack.

B. Sybil Attack

To control Sybil attack we have to change session key after specific time as well as reconfiguration of network devices. Physical protection of the network is also very important for prevention as well as detection of such attacks.

C. Wormhole

For prevention of wormhole attack there should be an efficient monitoring system that should monitor all the network devices. The monitoring system may use packet leaches for this purpose.

D. Spoofing and traffic Analysis

For detection and prevention of spoofing attacks regular monitoring of sensor nodes as well as sending of dummy packets when there is no traffic on the network. Another option is to use different routes to send confidential information.

E. Detection of Node Replication

B. Prano et al [17] proposed two techniques for detection of node replication in wireless sensor networks. i) Line selected multicast and ii) Randomized multicast. These techniques take the advantage of node broadcasting, where a sensor node propagates a broadcast message in the network. If a node receives a duplicate message it identifies the conflict and recognizes the duplicate node. Randomized multicast randomly chooses the two witnesses for replicated node, as compare to line selected multicast. However randomized multicast has more communication overhead.

F. Intrusion Detection

As compared to other attacks, intrusion detection is based on behavior of intruders. Detection of this attack is possible when intruder node start abnormal behavior as compare to normal sensor node. For this purpose the base station maintain a record of intruder signature and is able to identify an attacker and legitimate node.

G. Trust between Nodes

In such type of networks their may be certain level of trust, because traditional security techniques are not possible to implement in these networks due to limited energy, memory and computation power. Many authors proposed trust management techniques in these networks like H. Zahu et al [33] compute certain level of trust in wireless networks between different nodes. For this purpose they used authenticated transitive graph and transitive signature scheme. P. Zhang et al [34] developed a trust based security system for secure routing and data protection.

V. Security Protocols For Wireless Sensor Networks

In this section we discuss various protocols proposed for security of wireless sensor networks by different researchers.

A. SNEP Protocol

SNEP protocol [5] was designed as basic component of another protocol SPINS (Security protocol for wireless Sensor Networks) that was basically designed for secure key distribution in wireless sensor networks. SNEP define the primitives for authentication of sensor node, data confidentiality and data integrity. However the drawback of this protocol is lower data freshness. SNEP protocol uses shared counter for semantic confidentiality not initial vectors. Using SNEP the plain text is ciphered with CTR encryption algorithm. Both sender and receivers are responsible to update the shared counter once when they sent or receive cipher blocks [37]. There fore sending counter in message is not important, however every message has message authentication code (MAC). This is computed from cipher data with the help of CBC-MAC algorithm. When the receiver node receives data it recomputed MAC and compared with the received MAC. If both are same it means data received in the packet is right.

B. TESLA With Instant Key Disclosure (TIK)

Y. C. Hu et al [23] proposed TIK protocol for controlling wormhole attack. This protocol is used for authentication of nodes in broadcast communication. TIK is extended form of TESLA protocol and it works on the basis of temporal lashes (efficient symmetric cryptographic primitives) that help the receivers to detect a wormhole attack. Message authentication code is computed with symmetric cryptographic primitives. TIK needs that there should be complete time synchronization between sender and receiver as well as use a single public key for scalable key distribution. There are three stages in TIL protocol. i) Sender Setup: The sender uses a pseudo random function (PRF) to calculate master key and series of other keys. I also selects uniformly distributed points in time at which key is published like at T^0 disclose K^0, T^1 disclose K^1 and so on. ii) Receiver Bootstrapping: All nodes have synchronized clocks and each receiver knows every sender hash root as well as other associated parameters which help him to authenticate a sender node. iii) Sending and verifying packets: For verifying packets the sender node calculates a key before sending packets on the basis of arrival time at destination. Using that key sender also send a MAC code with packet. The key is still secret although packet is received at destination. After receiving packet the key is transferred toward destination if the packet is verified correctly the packet must have originates from the claimed user. However a drawback of this protocol is authentication delay the receiver has to wait for sender key to authenticate a packet.

C. Pair wise key per-Distribution Scheme

W. Du et al [24] proposed a pair wise key distribution scheme for wireless sensor networks. The proposed scheme is totally based on Blom's key pre distribution scheme which allows any pair of nodes in the network to find a pair wise secret key. Pair wise keys enable nodes authentication, increase network resilience and decrease communication and computation overhead. The author uses the concept of graph theory and draws an edge between two nodes if and only if they can find a secret key between themselves. There are few stages of pair wise key distribution scheme i. Key pre distribution phase in which key information is assigned to each node in the network. ii. Key agreement phase iii) Computing local connectivity and memory usage. This scheme is flexible and scalable as well as accepts the addition of new sensor nodes in later stages. However this scheme consumes more energy due to modular multiplication.

D. REWARD

Z. karakehayou [25] proposed a new algorithm know as REWARD for security against black hole attack as well as malicious nodes. It works on geographic routing. There are two different kinds of broadcast messages used by REWARD. MISS message helps in the identification of malicious sensor nodes. While the second message SAMBA is used to recognize the physical location of detected black hole attacks and broadcast that location. REWARD uses broadcast inter radio behavior to observe neighbor node's transmission and detect black hole attack. Whenever any sensor misbehaves it maintain a distributed database and save its information for future use. However the main drawback of this protocol is high energy consumption.

E. Tiny Sec

Tiny Sec protocol [26] was proposed by C. Karlof et al for secure communication in resource limited wireless sensor networks. There are two types of security options in Tiny Sec. i) Authenticated Encryption: In which the payload is encrypted
and message authentication code (MAC) is used to authenticate a data packet. Where message authentication code is itself computed from packet header. For payload encryption 8 byte initial vector (IV) is used with cipher block chain (CBC). ii) Authentication Mode: The main difference in this mode and encrypted mode is that payload is not encrypted in simple authentication mode although authentication is done with the help of message authentication code.

F. Secure Data Aggregation

B. Przydatek et al [27] developed a framework for secure information aggregation in wireless sensor networks. the author used few sensor nodes as aggregator. These nodes aggregate information request which help to decrease communication overhead. The aggregator shares its results with home server and performs efficient interactive proofs. Where home server will be able to ensure results and detect any misconduct or any aggregator involve in cheating. Whenever the aggregator results are not similar to the home server results, the home server will recognize the attacker. In large sensor networks a single aggregator cannot handle the whole network therefore the set of aggregator nodes are used in hierarchical manner.

G. Distributed MD Protocol / TDMA

L. F. W. Hoesel [28] proposed a TDMA based medium access protocol for wireless sensor networks. This protocol minimizes overhead on physical layer as well as reduces the number of transceiver switches. Medium access protocol is not dependent on any base station. Every sensor node in the network is independent to choose its own time slot. There is no need of handshaking mechanism before data transfer because the control message and data units are directly transferred after each other. This protocol provides security against sleep deprivation attack on sensor nodes.

H. Communication Security

S. Slijepcevic et al [29] proposed a communication security framework for wireless sensor networks. The author divided data packets into three categories i) Mobile code ii) Location of Sensor Node iii) Application specific data, as well as define a certain security level for these data types. The security strength depends on importance of information where level 1 is more strengthen then level 2 and level 3. For encryption of data RC6 algorithm is used with different number of rounds depending in the sensitivity of data. All nodes in the network use a set of master keys which depends on life time of the network. The whole network is divided into cells where sensor nodes with in one cell share a common location based key.

I. Statistical En-Route Filtering

F. Y. Haiyon et al [30] present a statistical en-route filtering technique to control attacks on compromised sensor nodes, where a compromised node can easily inject wrong report in the network that cause depletion of finite resources at sensor nodes as well as causes false alarms. Statistical En-Route Filtering is able to detect and destroy such false reports in the network. For this purpose message authentication code (MAC) is used to check the validity of each message. When sensed data is forwarded toward sink node each node in the middle verify that message. Statistical En-Route Filtering relies on collective information from multiple sensor nodes. When an event occurs the sensor nodes in the surrounding collectively generate a legitimate report that carries multiple message authentication codes (MAC's). The report is forwarded toward sink node and each node in the middle verifies the report with certain probability, when the report is found incorrect it is dropped. The probability of message incorrectness increases with number of hops. In many cases a false report may reaches to a sink node where sink node will be responsible to verify it again. However this approach causes delay as well as increase communication overhead and energy consumption in resource limited networks.

VI. Conclusion

Wireless sensor Networks have certain inherit limitations therefore instead of communication security it also needs a

fool proof physical security. Most common attack in such type of network is that node compromise to accept tempered information and forward it onward. Therefore cryptography is not enough to secure such networks. Sensor nodes authentication and encryption of information may make it more strengthened. In this paper we discussed security requirement for wireless sensor networks, we analyze different security threats and possible attacks as well as existing security approaches proposed by different researches with their basic characteristics. However attack detection and prevention is still an important research area in wireless sensor network.

REFERENCES

[1] N. Boudriga, A new scheme for mobility, sensing and security management in WSB" IEEE Annual simulation symposium (ANSS), 2006.
[2] J. Albath, S. Madaria, Practical Algorithms for Data Security (PADS) in wireless sensor networks Mobi-De 07, Beijing, China 2007.
[3] N. D. Vasumathyl, G. Velmathil, N.SkalavosII, On the Rijndael Encryption Algorithm Matalb Based implementation Department of Electronics and Communication Engineering, Sirsiva Subramania Nadar college of Engineering Tamalnadu, India, 2008.
[4] www.wikipedia.com ttp://en.wikipedia.org/wiki/Advanced Encryption Standard, Jan 2009.
[5] L. Tobarra, D. Cazorla, F. Cuartero, Formal Analysis of Sensor Network Encryption Protocol (SNEP) IEEE Internatonal Conference on Mobile Ad-hoc and Sensor Systems, MASS 2007, PISA, 8-11 Oct. 2007.
[6] S. Zhu, S. Setia, S. Jajodia, LEAP, Efficient Security Mechanism For Large Scale Distributed sensor Networks Proceeding of ACM Conference on Computer and Communication Security, (CSS,03) pp,62-72, 2003.
[7] M. Sherin. M. Yousef, A. Baith. Mohamd, mark A. Mikial, An Enhanced Security Architecture For Wireless Sensor Network Recent Advances on Data Networks, Communications, Computers, ISBN-1790-5109, Sep 2009.
[8] C. karlof, D. Wagner, Secure Routing in Wireless Sensor Networks, Attacks and Countermeasures Elsevier's Ad-hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, pp, 293-315, September 2003.
[9] B.J. Culpepper, H.C. Tseng, Sink hole intrusion indicators in DSR MANET's Proceeding of International Conference Broad Band Networks. PP, 681-688, 2004.
[10] Blackrert, W.J. Gregg, D.M. Castner, A. k. Kyle, E.M. Home, Jokerst. R.M, Analyzing Interaction between Distributed Denial of service Attacks and Mitigation Technoologies Proceeding of International Conference information Survivability and Exposition, DARPA, pp, 26-36, 22-24, April 2003.
[11] Wang. B.T, Schulzarinne.H, An IP Traceback Mechanism for Reflective DOS Attacks Canadian Conference on Electrical and Computer Engineering, pp, 901-904, 2-5, May 2004.
[12] Al-Sakib khan pathan, Hyung-Woo Lee, Choong Seon Hong, Security in Wireless Sensor Networks: Issues and Challenges International Conference ICACT-o6. 20-22 Feb, 2006.
[13] Douceur. J, The Sybil Attacks First International workshop on Peer to Peer Systems 2002.
[14] Newsome. J, Shi. E, Song. D, Perrig. A, The Sybil Attacks in sensor Networks Analysis and Defenses Proceeding of International Symposium on Information Processing in Sensor Networks, ACM, pp 269-268, 2004.
[15] Pfleeger C. P, Pleeger. S. L, security in Computing 3rd Edition Prentice Hall, 2003.
[16] Mona sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabdai, S. Beheshti "A Survey on Wireless Sensor Networks Security" International Conference Science of Electronics, Technologies of Information and Telecommunication, Tunisia, March 25-29, 2007.
[17] B. Parno, A. Perrig, V. Gligor, Distributed Detection of Node Replication Attacks in Sensor Networks Proceeding of IEEE Symposium on Security and Privacy, May 2005.
[18] R. Anderson, M. Khun, Low Cost Attacks on Tamper Resistant Devices International Workshop on security Protocols, LNCS-1997-98.
[19] Yang Xaio Security in Distributed, Grid and Pervasive Computing Auerbach Publications, CRC Press 2006.
[20] H. Yang, H. Luo, F. Ye, S. Lu, L. Zhang Security in Mobile Ad-hoc Networks: Challenges Solutions IEEE Wireless Communiaction, Vol-11, pp 38-47, Feb 2004.
[21] K. Sharma, m. K. Ghose, D. Kumar, R. P. Kumar, V. K. pandy, A Comparative Study of various Security Approaches used in wireless Sensor Networks International Journal of Advanced Science and Technology. Vol-17, April, 2010.
[22] S. Capkun and J. P. Hubaux Secure Positioning in Wireless Networks IEEE Journal on selected Areas in Communication, pp, 221-232, 2006.
[23] Y. C. Hu., A. Perrig, D. B. Johnson, Packet Leashes. A Defense against Wormhole Attacks in Wireless Networks 22nd Annual Conference of IEEE Computer and Communication Societies, IEEE ONFOCOM 2003, pp, 1976-1986, 3 April, 2003.
[24] W. Du, J. Deng, S. Han, P. K. Varshney, A Pairwise Key Pre-distribution scheme for Wireless Sensor Networks Proceeding of ACM international Conference on Computer and Communication Security, pp, 42-51, 2003.
[25] Z. Karakehayov, Using REWARD, to Detect Team Balckhole Attacks in Wireless sensor Networks Workshop on Real world Wireless Sensor Networks, (REAL WSN, 05) Stockholm, Swedan, June 2005.
[26] C. Karlof, N. Sandy, D. Wagner, TinySec: A Link Layer Security Architecture for Wireless Sensor Networks In Proceeding. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, pp. 162-175, 2004.
[27] B. Przydatek, D. Song, A. Perrig, SIA: Secure information aggregation in Sensor Networks Proceedings of International conference on Embedded Networked Sensor Systems.-ACM,-pp.-255-265,-2003.
[28] L. F. van Hoesel, P. J. Havinga, A Lightweight Medium Access Protocol (LMAC) for Wireless Sensor Networks Reducing Preamble Transmissions and Transceiver State Switches," in INSS, June 2004.
[29] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck, and M. B. Srivastava, On Communication Security in Wireless Ad-hoc Sensor Networks 11th IEEE International Workshops on Enabling Technologies, Infrastructure for Collaborative Enterprises, pp.139-144, 10-12 June, 2002.
[30] Fan. Ye, H. Luo, Songwu. Lu. L. Zhang. Statistical en-route Filtering of injected False Data in Sensor Networks IEEE Journal on Selected Areas in Communications, Vol-23, (4), pp. 839-850, April 2005.
[31] T. Aura, P. Nikader, J. Leiwo. DoS Resistant Authentication with Client Puzzels In Revised Papers from 8th International Workshop on security Protocols, pages 170-177, Springer, Verlag, 2001.
[32] A.D. Wood, J. A. Stankovic Denial of Service in Sensor Network Computer, IEEE, Volume 35, pp.54-62, Oct, 2002.
[33] H. Zhu, F. Bao, R.H.Deng, k. Kim Computing of Trust in Wireless Networks In proceeding of IEEE International Conference on Vehicular Technology, Los Angles, California, September 2004.
[34] Z. Yan, P. Zhang, T. Virtanen Trust Evaluation Based Security Solution in Ad-hoc Networks Proceeding of 7th Nordic Workshop on Secure IT System, 2003.
[35] H. Chan, A. Perrig, and D. X. Song, Random key pre-distribution schemes for Sensor Networks in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2003.

S.No	Security Protocol	Characteristics
1	SNEP [5]	Security from Spoofing attack, Low overhead, Message protection, weaker data freshness, Authentication of data.
2	Radio based Random Key Pre-distribution [14]	Security form sybil attack (detection and prevention), Verify Node's localization, Attestation, Pre distribution of key, Registration.
3	TIK [23]	Security from Wormhole attack, Based on Symmetric cryptography, Time Synchronization, Packet leashes. Expensive in computation, High energy Consumption.
4	Pair wise key per-Distribution [24]	Security from spoofing attack, Protection of Network, Resilience, Authentication of data and nodes, Per distribution of key.
5	REWARD [25]	Security from Black hole attack, Observe neighbor behavior, Geographic routing.
6	TinySec [26]	Security from Spoofing and reply back attack, Data integrity and confidentiality, Link layer, Message Authentication.
7	Aggregate Commit Prove Framework [27]	Security from Aggregation based attacks, High energy consumption, high traffic
8	Distributed MD Protocol/TDMA [28]	Control sleep deprivation attack, listen and control interval jamming, lower throughput, not suitable for multihop networks, Hidden nodes problem, dynamic synchronization, different duty cycle.
9	Communication Security [29]	Security against information spoofing, Lower energy consumption, protect the network even after attack in some regions.
10	Statistical En-Route Filtering [30]	Security against information spoofing, detection and prevention of false routing reports.