IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

Collaborative Distributed Protocol and Holistic Approach of Security in Wireless Sensor Networks

[1] **Chandramohan.S;** [2] **Pavithra.M;** [3] **Sindhu.B**

[1] Rathinam Technical Campus, Eachanri,
Rathinam Techzone, Coimbatore

[2] Rathinam Technical Campus, Eachanri,
Rathinam Techzone, Coimbatore

[3] Rathinam Technical Campus, Eachanri,
Rathinam Techzone, Coimbatore

Abstract - Wireless Sensor Network (WSN) is the most employed network service in commercial and industrial applications, for the ease of its technical development in a processor, communication, and low-power usage of embedded computing devices. Sensor nodes are used for constant sensing, event ID, event detection & local control of actuators. The applications of WSN mainly include health, military, environmental, smart home technology, & other commercial areas. When deployed in hostile environmental conditions, the sensor nodes are vulnerable to physical capture and other constraints that puts security as a major challenge for the researcher's in the field of computer networking. The inclusion of wireless communication technology also incurs various types of security threats. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks. We also discuss the holistic view of security for ensuring layered and robust security in wireless sensor networks.

Keywords -*Wireless Sensor Network, Security, Denial of Service (DoS), Intrusion Detection System (IDS), Authentication, Sensor, Attacks, Holistic Approach*

1. Introduction

In today's realistic world Wireless Sensor Networks (WSN) [1] has become the most popular communication medium because of its low cost architecture. It is one of the emerging wireless networks among the various classes of communication networks such as Cellular Networks, Adhoc Networks and Mesh Networks. An adhoc network cannot be considered as a sensor network because an adhoc Network uses multi hop radio relaying and is lack of sensors [2]. The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, over a specific geographic area for some specific purposes like target tracking, surveillance, environmental monitoring etc. Today's sensors can monitor temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects, and other properties [4]. In case of wireless sensor network, the communication among the sensors is done using wireless transceivers. The attractive features of the wireless sensor networks attracted many researchers to work on various issues related to these types of networks. However, while the routing strategies and wireless sensor network modeling are getting much preference, the security issues are yet to receive extensive focus. In this paper, we explore the security issues and challenges for next generation wireless sensor networks and discuss the crucial parameters that require extensive investigations for enhancements.

2. Architecture of a Wireless Sensor Network

A WSN is a collection of sensor nodes which are deployed in a sensor fields which collect and route data back to the Base Station. A sensor node can be divided into four basic parts, viz. the sensing unit, a processing unit, a transceiver unit, and a power unit [7][8]. Localization is the heart of the routing principle in WSN. The position finding system helps the sensor node to discover its position in the environment. The power unit gives the constant power supply to the sensor nodes which is the prime target area of the intruders.

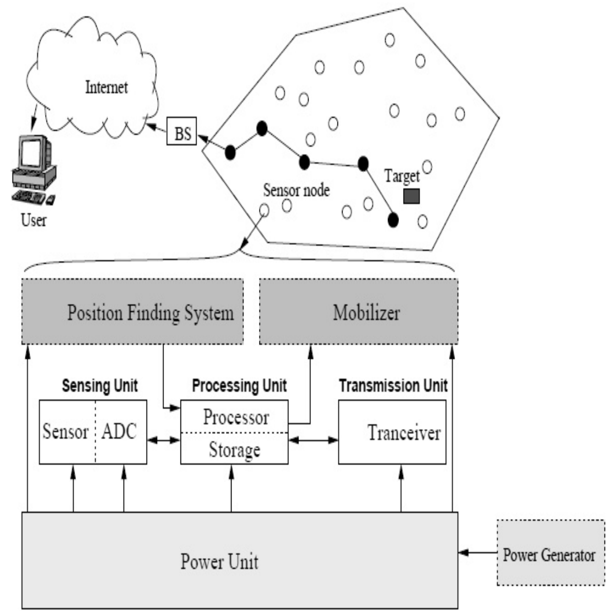

Figure 1. The components of a sensor node (Source: [7]).

These issues are well-enumerated in some past researches [16], [17], [18] and also a number of security schemes are already being proposed to fight against them. However, the security mechanisms devised for wireless ad hoc networks could not be applied directly for wireless sensor networks because of the architectural disparity of the two networks. While ad hoc networks are self-organizing, dynamic topology, peer to peer networks formed by a collection of mobile nodes and the centralized entity is absent [19]; the wireless sensor networks could have a command node or a base station (*centralized entity, sometimes termed as sink*).

The architectural aspect of wireless sensor network could make the employment of a security schemes little bit easier as the base stations or the centralized entities could be used extensively in this case. Nevertheless, the major challenge is induced by the constraint of resources of the tiny sensors. In many cases, sensors are expected to be deployed arbitrarily in the enemy territory (especially in military reconnaissance scenario) or over dangerous or hazardous areas. Therefore, even if the base station (sink) resides in the friendly or safe area, the sensor nodes need to be protected from being compromised

3. Understanding the Threats and Issues in Wireless Sensor Networks

Most of the threats and attacks against security in wireless networks are almost similar to their wired counterparts while some are exacerbated with the inclusion of wireless connectivity. In fact, wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. The broadcast nature of the wireless communication is a simple candidate for eavesdropping. In most of the cases various security issues and threats related to those we consider for wireless ad hoc networks are also applicable for wireless sensor networks.

3.1. Attacks in Wireless Sensor Networks

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Some of the existing major attacks in wireless sensor networks are pointed out.

3.1.1 Denial of Service

Denial of Service (DoS) [20], [21] is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing, misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

3.1.2 Attacks on Information in Transit

In a sensor network, sensors monitor the changes of specific parameters or values and report to the sink according to the requirement. While sending the report, the information in transit may be altered, spoofed, replayed again or vanished. As wireless communication is vulnerable to eavesdropping, any attacker can monitor the traffic flow and get into action to interrupt, intercept, modify or fabricate [22] packets thus, provide wrong information to the base stations or sinks. As sensor nodes typically have short range of transmission and scarce

IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

resource, an attacker with high processing power and larger communication range could attack several sensors at the same time to modify the actual information during transmission.

3.1.3 Sybil Attack

In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes (Figure 2). This type of attack where a node forges the identities of more than one node is the Sybil attack. [23], [24]. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection. [24].

Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols. Douceur [23] showed that, without a logically centralized authority, sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. However, detection of sybil nodes in a network is not so easy. Newsome et. al. [24] used radio resource testing to detect the presence of sybil node(s) in sensor network and showed that the probability to detect the existence of a sybil node is:

$$Pr(detection) = 1-(1-\sum_{all S,M,G} \frac{\binom{s}{S}\binom{m}{M}\binom{g}{G}}{\binom{n}{c}} \frac{S-(m-M)}{c})^{r}$$

Where, n is the number of nodes in a neighbor set, s is the number of sybil nodes, m malicious nodes, gnumber of good nodes, cis the number of nodes that can be tested at a time by a node, of which S are sybil nodes, M are malicious (faulty) nodes, G are good (correct) nodes and r is the number of rounds to iterate the test.

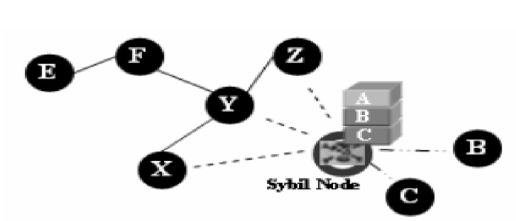

Figure 2: Sybil Attack

3.1.4 Black hole/Sinkhole Attack

In this attack, a malicious node acts as a black hole [25] to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them.

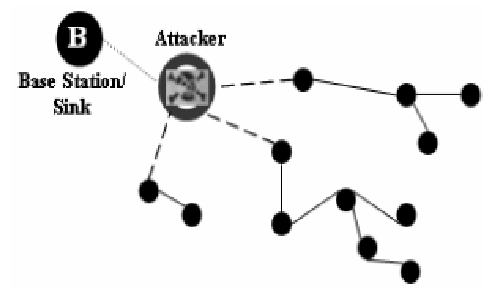

Figure 3Theconceptual view of a black hole/sinkhole attack

3.1.5 Hello Flood Attack

Hello Flood Attack is introduced in [26]. This attack uses HELLO packets as a weapon to convince the sensors in WSN.In this sort of attack an attacker with a high radio transmission (termed as a laptop-class attacker in [26]) range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbor. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbor and are ultimately spoofed by the attacker.

3.1.6 Wormhole Attack

Wormhole attack [27] is a critical attack in which the attacker records the packets (or bits) at one location in the network and tunnels those to another location. The tunneling or retransmitting of bits could be done selectively. Wormhole attack is a significant threat to wireless sensor networks, because; this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover the neighboring information. In fact, this attack can affect even the nodes those are considerably far from the base stations

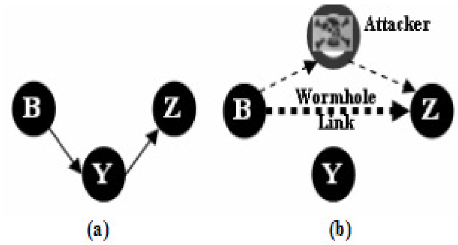

Figure 4: Wormhole Attack

Figure 4 (a and b) shows a situation where a wormhole attack takes place. When a node B (for example, the base station or any other sensor) broadcasts the routing request packet, the attacker receives this packet and replays it in its neighborhood. Each neighboring node receiving this replayed packet will consider itself to be in the range of Node B, and will mark this node as its parent. Hence, even if the victim nodes are multihop apart from B, attacker in this case convinces them that B is only a single hop away from them, thus creates a wormhole.

Table 1: Summary of various security schemes for wireless sensor networks

Security schemes	Attacks Deterred	Network Architecture	Major Features
JAM [38]	DoS Attack (Jamming)	Traditional wireless sensor network	Avoidance of jammed region by using coalesced neighbor nodes
Wormhole based [39]	DoS Attack (Jamming)	Hybrid (mainly wireless partly wired) sensor network	Uses wormholes to avoid jamming
Statistical En-Route Filtering [33]	Information Spoofing	Large number of sensors, highly dense wireless sensor network	Detects and drops false reports during forwarding process
Radio Resource Testing, Random Key Pre-distribution etc. [24]	Sybil Attack	Traditional wireless sensor network	Uses radio resource, Random key pre-distribution, Registration procedure, Position verification and Code attestation for detecting Sybil entity
Bidirectional Verification, Multi-path multi-base station routing [40]	Hello Flood Attack	Traditional wireless sensor network	Adopts probabilistic secret sharing, Uses bidirectional verification and multi-path multi-base station routing
On Communication Security [32]	Information or Data Spoofing	Traditional wireless sensor network	Efficient resource management, Protects the network even if part of the network is compromised
TIK [27]	Wormhole Attack, Information or	Traditional wireless sensor network	Based on symmetric cryptography, Requires accurate time synchronization between all

	Data Spoofing		communicating parties, implements temporal leashes
Random Key Predistribution [29], [30], [41]	Data and information spoofing, Attacks in information in Transit	Traditional wireless sensor Network	Provide resilience of the network, Protect the network even if part of the network is compromised, Provide authentication measures for sensor nodes
[42]	Data and Information Spoofing	Distributed Sensor Network, Large-scale wireless sensor network with dynamic nature	Suitable for large wireless sensor networks which allows addition and deletion of sensors, Resilient to sensor node capture

4. Proposed Security Schemes and Related Work

In the recent years, wireless sensor network security has been able to attract the attentions of a number of researchers around the world. In this section we review and map various security schemes proposed or implemented so far for wireless sensor networks.

4.1. Security Schemes for Wireless Sensor Networks

[26] gives an analysis of secure routing in wireless sensor networks. [34] studies how to design secure distributed sensor networks with multiple supply voltages to reduce the energy consumption on computation and therefore to extend the network's life time. [7] aims at increasing energy efficiency for key management in wireless sensor networks and uses Younis et. al. [36] network model for its application. Wood et al. [31] studies DoS attacks against different layers of sensor protocol stack. JAM [38] presents a mapping protocol which detects a jammed region in the sensor network and helps to avoid the faulty region to continue routing within the network, thus handles DoS attacks caused by jamming.

In [39] the authors show that wormholes those are so far considered harmful for WSN could effectively be used as a reactive defense mechanism for preventing jamming DoS attacks. Ye et. al. [33] presents a statistical en route filtering (SEF) mechanism to detect injected false data in sensor network and focus mainly on how to filter false data using collective secret and thus preventing any single compromised node from breaking the entire system. SNEP & μTESLA [6] are two secure building blocks for providing data confidentiality, data freshness and broadcast authentication.

TinySec [35] proposes a link layer security mechanism for sensor networks which uses an efficient symmetric key encryption protocol. Newsome et. al. [24] proposes some defense mechanisms against sybil attack in sensor networks. Kulkarni et al. [28] analyzes the problem of assigning initial secrets to users in ad-hoc sensor networks to ensure authentication and privacy during their communication and points out possible ways of sharing the secrets. presents a probabilistic secret sharing protocol to defend Hello flood attacks. The scheme uses a bidirectional verification technique and also introduces multi-path multi-base station routing if bidirectional verification is not sufficient to defend the attack. REWARD [43] is a routing algorithm which fights against black holes in the network. [32] proposes separate security schemes for data with various sensitivity levels and a location-based scheme for wireless sensor networks that protects the rest of the network, even when parts of the network are compromised. [27] implements symmetric key cryptographic algorithms with delayed key disclosure on motes to establish secure communication channels between a base station and sensors within its range. [41], [42], [29] and [30] propose key pre-distribution schemes, which target to improve the resilience of the network. In Table 1 we summarize various security schemes along

IJCSN - International Journal of Computer Science and Network, Volume 6, Issue 3, June 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

with their main properties proposed so far for wireless sensor networks.

4.2 Proposed Methodology

A holistic approach [37] aims at improving the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer might not be an efficient solution rather employing a holistic approach could be the best option.

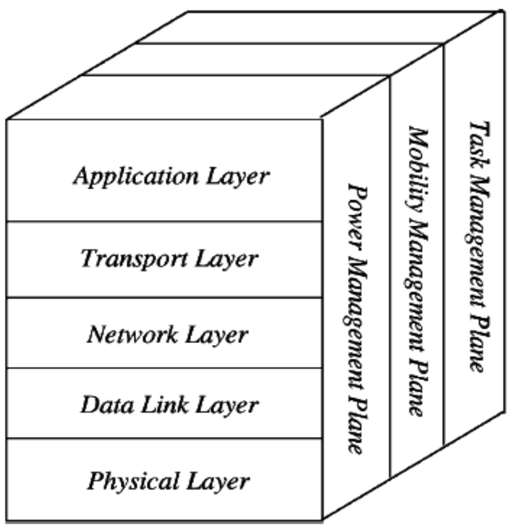

Figure 5: Holistic view of Security in wireless sensor networks

The holistic approach has some basic principles like, in a given network; security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not surpass the assessed security risk at a specific time, if there is no physical security ensured for the sensors, The security measures must be able to exhibit a graceful degradation if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measures should be developed to work in a decentralized fashion.

If security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers. By building security layers as in the holistic approach, protection could be established for the overall network.

4.3Collaborative Distributed Protocol

A Collaborative distributed protocol that leverages sensor cooperation and Locomotion to achieve probabilistic Key insulation. Sensors take advantage of mobility attains better security.

Many current and envisaged applications for wireless sensor Networks (WSNs) involve data Collection in remote, inaccessible or hostile environments, such as deserts, mountains, ocean floors, and battle fields. A multitude of sensors might Be deployed within a certain Area and their activity is usually monitored and managed by a powerful trusted entity using both analytical and simulation results, we show that the proposed protocol provides probabilistic key insulation without any trusted third parties or secure hardware and with minimal overhead.

A constant storage self –healing protocol for WSNs. Sensor key Update uses a polynomial –based Secret sharing scheme, performed with the help of the sink. The sink periodically broadcasts information to allow non revoked Sensors to update their current Session key. Based on the time of corruption, the security state of a given sensor can be partitioned in three epochs:

1.Time before corruption;
2.Time during corruption; and
3.Time following corruption

Nothing can be done about security in epoch 2 as the adversary controls the sensor, while enforcing security in epochs 1 and 3 requires forward and backward secrecy, respectively. Informally, a cryptographic protocols forward secured if exposure of secret material at a given time does not lead to compromise of secrets for any time preceding compromise. Whereas, a cryptographic protocol is backward secure if compromise of secret material at a given time does not lead to compromise of any secret to be used in future.

5. Conclusion

Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. However, developing such a detection mechanism and making it efficient represents a great research challenge. Trust management mechanism, as an important complement for password-based system, has significant advantages for the WSN in the settlement of internal attack, identifying malicious nodes, system security and reliability improvement, and so on. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models. As there is a lack of combined effort to take a common model to ensure security for each layer, in future though the security mechanisms become well-established for each individual layer, combining all the mechanisms together for making them work in collaboration with each other will incur a hard research challenge. Even if holistic security could be ensured for wireless sensor networks, the cost-effectiveness and energy efficiency to employ such mechanisms could still pose great research challenge in the coming days.

References

[1] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[2] Akylidiz, I. F., Su, W., Sankarasubramaniam, Y, and Cayirci, E., "Wireless Sensor Networks: A Survey", Computer Networks, 38, 2002, pp. 393-422.

[3] Dai, S, Jing, X, and Li, L, "Research and analysis on routing protocols for wireless sensor networks", Proc. International Conference on Communications, Circuits and Systems, Volume 1, 27-30 May, 2005, pp. 407-411.

[4] Pathan, A-S. K., Islam, H. K., Sayeed, S. A., Ahmed, F. and Hong, C. S., "A Framework for Providing E-Services to the Rural Areas using Wireless Ad Hoc and Sensor Networks", to appear in IEEE ICNEWS 2006.

[5] Undercoffer, J., Avancha, S., Joshi, A., and Pinkston, J., "Security for Sensor Networks", CADIP Research Symposium, 2002, available at,http://www.cs.sfu.ca/~angiez/personal/paper/sensor-ids.pdf

[6] Perrig, A., Szewczyk, R., Wen, V., Culler, D., and Tygar, J. D., "SPINS: Security Protocols for SensorNetworks", Wireless Networks, vol. 8, no. 5, 2002, pp. 521-534.

[7] Jolly, G., Kuscu, M.C., Kokate, P., and Younis, M., "A Low-Energy Key Management Protocol for Wireless Sensor Networks", Proc. Eighth IEEE International Symposium on Computers and Communication, 2003. (ISCC 2003). vol.1, pp. 335 - 340.

[8] Rabaey, J.M., Ammer, J., Karalar, T., Suetfei Li., Otis, B., Sheets, M., and Tuan, T., "PicoRadios for wireless sensor networks: the next challenge in ultra-low power design"2002 IEEE International Solid-State Circuits Conference (ISSCC 2002), Volume 1, 3-7 Feb. 2002, pp. 200 – 201.

[9] Hollar, S, "COTS Dust", Master's Thesis, Electrical Engineering and Computer Science Department, UC Berkeley, 2000.

[10] Saleh, M. and Khatib, I. A., "Throughput Analysis of WEP Security in Ad Hoc Sensor Networks", Proc. The Second International Conference on Innovations in Information Technology (IIT'05), September 26-28, Dubai, 2005.

[11] Kurak, C and McHugh, J, "A Cautionary Note on Image Downgrading in Computer Security Applications", Proceedings of the 8th Computer Security Applications Conference, San Antonio, December, 1992, pp. 153-159.

[12] Mokowitz, I. S., Longdon, G. E., and Chang, L., "A New Paradigm Hidden in Steganography", Proc.of the 2000 workshop on New security paradigms, Ballycotton, County Cork, Ireland, 2001, pp. 41 – 50.

[13] Kim, C. H., O, S. C., Lee, S., Yang, W. I., and Lee, H-W., "Steganalysis on BPCS Steganography", Pacific Rim Workshop on Digital Steganography (STEG'03), July 3-4, Japan , 2003.

[14] Younis, M., Akkaya, K., Eltoweissy, M., and Wadaa, A., "On handling QoS traffic in wireless sensor networks", Proc. of the 37th Annual Hawaii International Conference on System Sciences, 2004, 5-8 January, 2004, pp. 292 – 301.

[15] Orihashi, M., Nakagawa, Y., Murakami, Y., and Kobayashi, K., "Channel synthesized modulation employing singular vector for secured access on physical layer", IEEE GLOBECOM 2003, Volume 3, 1-5 December, 2003, pp. 1226 – 1230.

[16] Zhou, L. and Haas, Z. J., "Securing ad hoc networks", IEEE Network, Volume 13, Issue 6, Nov.-Dec. 1999, pp. 24 – 30.

[17] Strulo, B., Farr, J., and Smith, A., "Securing Mobile Ad hoc Networks — A Motivational Approach", BT Technology Journal, Volume 21, Issue 3, 2003, pp. 81 – 89.

[18] Yang, H., Luo, H., Ye, F., Lu, S., and Zhang, L., "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, Volume 11, Issue 1, February 2004, pp. 38 – 47.

[19] Pathan, A-S. K., Alam, M., Monowar, M., and Rabbi, F., "An Efficient Routing Protocol for Mobile Ad Hoc Networks with Neighbor Awareness and Multicasting", Proc. IEEE E-Tech, Karachi, 31 July, 2004, pp. 97-100.

[20] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 36.

[21] Wang, B-T. and Schulzrinne, H., "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.

[22] Pfleeger, C. P. and Pfleeger, S. L., "Security in Computing", 3rd edition, Prentice Hall 2003.

[23] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems (2002).

[24] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[25] Culpepper, B.J. and Tseng, H.C., “Sinkhole intrusion indicators in DSR MANETs”, Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.
[26] Karlof, C. and Wagner, D., “Secure routing in wireless sensor networks: Attacks and countermeasures”, Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.
[27] Hu, Y.-C., Perrig, A., and Johnson, D.B., “Packet leashes: a defenseagainst 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.
[28] Kulkarni, S. S., Gouda, M. G., and Arora, A., “Secret instantiation in adhoc networks,” Special Issue of Elsevier Journal of Computer Communications on Dependable Wireless Sensor Networks, May 2005, pp. 1–15.
[29] Du, W., Deng, J., Han, Y. S., and Varshney, P. K., “A pairwise key pre-distribution scheme for wireless sensor networks”, Proc. of the 10th ACM conference on Computer and communications security, 2003, pp. 42-51.
[30] Oniz, C. C, Tasci, S. E, Savas, E., Ercetin, O., and Levi, A, “SeFER: Secure, Flexible and EfficientRouting Protocol for Distributed Sensor Networks”, from http://people.sabanciuniv.edu/~levi/SeFER_EWSN.pdf
[31] Wood, A. D. and Stankovic, J. A., “Denial of Service in Sensor Networks”, Computer, Volume 35, Issue 10, Oct. 2002 pp. 54 - 62.
[32] Slijepcevic, S., Potkonjak, M., Tsiatsis, V., Zimbeck, S., and Srivastava, M.B., “On communication security in wireless ad-hoc sensor networks”, 11th IEEE International Workshops on EnablingTechnologies: Infrastructure for Collaborative Enterprises, 2002, 10-12 June 2002, pp. 139 – 144.
[33] Ye, F., Luo, H., Lu, S, and Zhang, L, “Statistical en-route filtering of injected false data in sensor networks”, IEEE Journal on Selected Areas in Communications, Volume 23, Issue 4, April 2005, pp. 839 – 850.
[34] Yuan, L. and Qu, G., “Design space exploration for energy-efficient secure sensor network”, Proc.The IEEE International Conference on Application-Specific Systems, Architectures and Processors, 2002, 17-19 July 2002, pp. 88 – 97.
[35] Karlof, C., Sastry, N., and Wagner, D., “TinySec: a link layer security architecture for wireless sensor networks”, Proc. of the 2nd international conference on Embedded networked sensor systems, Baltimore, MD, USA, 2004, pp. 162 – 175.
[36] Younis, M., Youssef, M., and Arisha, K., “Energy-aware routing in cluster-based sensor networks” Proc. 10th IEEE International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 1-16 Oct. 2002 pp. 129 – 136.
[37] Avancha, S, “A Holistic Approach to Secure Sensor Networks”, PhD Dissertition, University of Maryland, 2005.
[38] Wood, A.D., Stankovic, J.A., and Son, S.H., “JAM: A Jammed-Area Mapping Service for Sensor Networks”, 24th IEEE Real-Time Systems Symposium, RTSS 2003, pp. 286-297.
[39] Cagalj, M., Capkun, S., and Hubaux, J-P., “Wormhole-based Anti-Jamming Techniques in SensorNetworks” from http://lcawww.epfl.ch/Publications/Cagalj/CagaljCH05-worm.pdf
[40] Hamid, M. A., Rashid, M-O., and Hong, C. S., “Routing Security in Sensor Network: Hello Flood Attack and Defense”, to appear in IEEE ICNEWS 2006, 2-4 January, Dhaka.
[41] Chan, H, Perrig, A., and Song, D., "Random key predistribution schemes for sensor networks", In IEEE Symposium on Security and Privacy, Berkeley, California, May 11-14 2003, pp. 197–213. http://people.sabanciuniv.edu/~levi/SeFER_EWSN.pdf
[42] Eschenauer, L. and Gligor, V. D., "A key-management scheme for distributed sensor networks", Proc. ACM CCS'02, 18-22 November 2002, pp. 41-47.
[43] 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, SwedenThe IEEE International Conference on Application-Specific Systems,Architectures and Processors, 2002, 17-19 July 2002, pp. 88 – 97.

Chandramohan.S received the B. Tech & M. Tech degrees from Anna University in 2009 & 2013, respectively. He worked as Assistant professor in AVS Engineering college, Salem from 2010 to 2011. After he worked as Assistant professor in VSB Engineering college, Coimbatore from 2012 to 2016.He has been Assistant professor in Rathinam Technical campus, Coimbatore since 2016.His research interest includes security in wireless sensor networks.

Pavithra.M received the B.E & M.E degrees from Avinashilingham University in 2014 & 2016, respectively. He has been Assistant professor in Rathinam Technical campus, Coimbatore since 2016.His research interest includes security in wireless sensor networks.

Sindhu.B received the B.E & M.E degrees from Anna University in 2010 & 2014, respectively. He worked as Assistant professor in Narayana Guru Engineering college, Coimbatore from 2011 to 2015. After he worked as Assistant professor in VSB Engineering college, Coimbatore from 2015 to 2016.He has been Assistant professor in Rathinam Technical campus, Coimbatore since 2016.His research interest includes security in wireless sensor networks.