Security in Wireless Sensor Networks: Issues and Challenges

Pulkit Berwal
Electronics and Communication Department

Abstract—Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. Wireless sensor networks require the need for effective security mechanisms. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. The inclusion of wireless communication technology also incurs various types of security threats. However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network/computer security. There is currently enormous research potential in the field of wireless sensor network security. Thus, familiarity with the current research in this field will benefit researchers greatly. This paper is an attempt to present a survey on the major topics in wireless sensor network security, and also present the obstacles and the requirements in the sensor security, classify many of the current attacks, and finally list their corresponding defensive measures.

Keywords—Sensor, Security, Attack, Holistic, Challenge, localization, authentication, attacks, broadcasting and multicasting, secure multicasting

I. INTRODUCTION
This Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors [1], [2], [3]. 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. Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the This work was supported by MIC and ITRC Project size of sensors, consequently the processing power, memory and type of tasks expected from the sensors. We discuss these issues and challenges in this paper. To address the critical security issues in wireless sensor networks we talk about cryptography, steganography and other basics of network security and their applicability in Section 2. We explore various types of threats and attacks against wireless sensor network in Section 3. Section 4 reviews the related works and proposed schemes concerning security in WSN and also introduces the view of holistic security in WSN. Finally Section 5 concludes the paper delineating the research challenges and future trends toward the research in wireless sensor network security.

II. OBSTACLE TO SENSOR SECURITY
A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. First, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. Second, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack. And third, sensor networks interact closely with their physical environments and with people, posing new security problems. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first [6].

A. Very Limited Resources
First, All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor. The major parameters are: Limited Memory and Storage Space: A sensor is a tiny device with only a small amount of memory and storage space for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm. For example, one common sensor type (TelosB) has an 16-bit, 8 MHz RISC CPU with only 10K RAM, 48K program memory, and 1024K flash storage [14]. With such a limitation, the software built for the sensor must also be quite small. Power Limitation: Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged.
(high cost of sensors). Therefore, the battery charge taken with them to the field must be conserved to extend the life of the individual sensor node and the entire sensor network.

B. Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication. The major parameters are: Unreliable Transfer: Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Packets may get damaged due to channel errors or dropped at highly congested nodes. The result is lost or missing packets. Furthermore, the unreliable wireless communication channel also results in damaged packets. Conflicts: Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem. More details about the effect of wireless communication can be found at [1]. Latency: The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes. The synchronization issues can be critical to sensor security where the security mechanism relies on critical event reports and cryptographic key distribution.

C. Unattended Operations

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes: Exposure to Physical Attacks: The sensor may be deployed in an environment open to adversaries, bad weather, and so on. The likelihood that a sensor suffers a physical attack in such an environment is therefore much higher than the typical PCs, which is located in a secure place and mainly faces attacks from a network. Managed Remotely: Remote management of a sensor network makes it virtually impossible to detect physical tampering (i.e., through tamperproof seals) and physical maintenance issues (e.g., battery replacement). Perhaps the most extreme example of this is a sensor node used for remote reconnaissance missions behind enemy lines. In such a case, the node may not have any physical contact with friendly forces once deployed. No Central Management Point: A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

III. FEASIBILITY OF BASIC SECURITY SCHEMES IN WIRELESS

Before Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, nonrepudiation, and anti-playback [5]? The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased. For the secure transmission of various types of information over networks, several cryptographic, steganographic and other techniques are used which are well known. In this section, we discuss the network security fundamentals and how the techniques are meant for wireless sensor networks.

A. Cryptography

The encryption-decryption techniques devised for the traditional wired networks are not feasible to be applied directly for the wireless networks and in particular for wireless sensor networks. WSNs consist of tiny sensors which really suffer from the lack of processing, memory and battery power [6], [7], [8], [9]. Applying any encryption scheme requires transmission of extra bits, hence extra processing, memory and battery power which are very important resources for the sensors’ longevity. Applying the security mechanisms such as encryption could also increase delay, jitter and packet loss in wireless sensor networks [10]. Moreover, some critical questions arise when applying encryption schemes to WSNs like, how the keys are generated or disseminated. How the keys are managed, revoked, assigned to a new sensor added to the network or renewed for ensuring robust security for the network. As minimal (or no) human interaction for the sensors, is a fundamental feature of wireless sensor networks, it becomes an important issue how the keys could be modified time to time for encryption. Adoption of pre-loaded keys or embedded keys could not be an efficient solution.

B. Steganography

While cryptography aims at hiding the content of a message, steganography [11], [12] aims at hiding the existence of the message. Steganography is the art of covert communication by embedding a message into the multimedia data (image, sound, video, etc.) [13]. The main objective of steganography is to modify the carrier in a way that is not perceptible and hence, it looks just like ordinary. It hides the existence of the covert channel, and furthermore, in the case that we want to send a secret data without sender information or when we want to distribute secret data publicly, it is very useful. However, securing wireless sensor networks is not directly related to steganography and processing multimedia data (like audio, video) with the inadequate resources [14] of the sensors is difficult and an open research issue.

C. Physical Layer Secure Access

Physical layer secure access in wireless sensor networks could be provided by using frequency hopping. A dynamic combination of the parameters like hopping set (available frequencies for hopping), dwell time (time interval per hop) and hopping pattern (the sequence in which the frequencies from the available hopping set is used) could be used with a little expense of memory, processing and energy resources.
Important points in physical layer secure access are the efficient design so that the hopping sequence is modified in less time than is required to discover it and for employing this both the sender and receiver should maintain a synchronized clock. A scheme as proposed in [15] could also be utilized which introduces secure physical layer access employing the singular vectors with the channel synthesized modulation.

IV. SECURITY REQUIREMENTS

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. Therefore, we can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks.

A. Data Confidentiality

Data confidentiality is the most important issue in network security. Every network with any security focus will typically address this problem first. In sensor networks, the confidentiality relates to the following [6]:

- A sensor network should not leak sensor readings to its neighbors. Especially in a military application, the data stored in the sensor node may be highly sensitive.
- In many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.
- Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks.

B. Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn’t mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

C. Data Freshness

Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. Typically shared keys need to be changed over time. However, it takes time for new shared keys to be propagated to the entire network. In this case, it is easy for the adversary to use a replay attack. Also, it is easy to disrupt the normal work of the sensor, if the sensor is unaware of the new key change time. To solve this problem a nonce, or another time-related counter, can be added into the packet to ensure data freshness.

D. Availability

Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What’s more, some approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. But all these approaches weaken the availability of a sensor and sensor network for the following reasons:

- Additional computation consumes additional energy. If no more energy exists, the data will no longer be available.
- Additional communication also consumes more energy. What’s more, as communication increases so too does the chance of incurring a communication conflict.
- A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network.

E. Self Organization

A wireless sensor network is a typically an ad hoc network, which requires every sensor node be independent and flexible enough to be self-organizing and self-healing according to different situations. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature brings a great challenge to wireless sensor network security as well.

F. Time Synchronization

Most sensor network applications rely on some form of time synchronization. In order to conserve power, an individual sensor’s radio may be turned off for periods of time. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair-wise sensors. A more collaborative sensor network may require group synchronization for tracking applications, etc.

G. Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals, etc.
H. Authentication

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). From the above, we can see that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the message authentication code (MAC) of all communicated data.

V. ATTACKS

Sensor networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, physical attacks, and so on. Denial of service attacks on wireless sensor networks can range from simply jamming the sensor’s communication channel to more sophisticated attacks designed to violate the 802.11 MAC protocol or any other layer of the wireless sensor network. Due to the potential asymmetry in power and computational constraints, guarding against a well-orchestrated denial of service attack on a wireless sensor network can be nearly impossible. A more powerful node can easily jam a sensor node and effectively prevent the sensor network from performing its intended duty. We note that attacks on wireless sensor networks are not limited to simply denial of service attacks, but rather encompass a variety of techniques including node takeovers, attacks on the routing protocols, and attacks on a node’s physical security. In this section, we first address some common denial of service attacks and then describe additional attacking, including those on the routing protocols as well as an identity based attack known as the Sybil attack. The most popular types of attacks are:

- Denial of Service Attacks
- The Sybil Attack
- Traffic Analysis Attack
- Node Replication Attack
- Attacks against Privacy
- Physical Attacks

VI. DEFENCE MEASURES

Now we are in a position to describe the measures for satisfying security requirements, and protecting the sensor network from attacks. We start with key establishment in wireless sensor networks, which lays the foundation for the security in a wireless sensor network, followed by defending against DoS attacks and secure broadcasting and multicasting.

A. Key Establishment

One security aspect that receives a great deal of attention in wireless sensor networks is the area of key management. Wireless sensor networks are unique (among other embedded wireless networks) in this aspect due to their size, mobility and computational/power constraints. Indeed, researchers envision wireless sensor networks to be orders of magnitude larger than their traditional embedded counterparts. This, coupled with the operational constraints described previously, makes secure key management an absolute necessity in most wireless sensor network designs. Because encryption and key management/establishment are so crucial to the defense of a wireless sensor network, with nearly all aspects of wireless sensor network defenses relying on solid encryption, we first begin with an overview of the unique key and encryption issues surrounding wireless sensor networks before discussing more specific sensor network defenses.

B. Defending against DoS Attacks

Since denial of service attacks is so common, effective defenses must be available to combat them. One strategy in defending against the classic jamming attack is to identify the jammed part of the sensor network and effectively route around the unavailable portion. Wood and Stankovic describe a two phase approach where the nodes along the perimeter of the jammed region report their status to their neighbors who then collaboratively define the jammed region and simply route around it. To handle jamming at the MAC layer, nodes might utilize a MAC admission control that is rate limiting. This would allow the network to ignore those requests designed to exhaust the power reserves of a node. This, however, is not fool-proof as the network must be able to handle any legitimately large traffic volumes. Overcoming rogue sensors that intentionally misroute messages can be done at the cost of redundancy. In this case, a sending node can send the message along multiple paths in an effort to increase the likelihood that the message will ultimately arrive at its destination. This has the advantage of effectively dealing with nodes that may not be malicious, but rather may have simply failed as it does not rely on a single node to route its messages. To overcome the transport layer flooding denial of service attack Aura, Nikander and Leiwo suggest using the client puzzles posed by Juels and Brainard in an effort to discern a node’s commitment to making the connection by utilizing some of their own resources. Aura et al. advocate that a server should force a client to commit its own resources first. Further, they suggest that a server should always force a client to commit more resources up front than the server. This strategy would likely be effective as long as the client has computational resources comparable to those of the server.
C. Secure Broadcasting and Multicasting

The research community of wireless sensor networks has progressively reached a consensus that the major communication pattern of wireless sensor networks is broadcasting and multicasting, e.g., 1-to-N, N-to-1, and M-to-N, instead of the traditional point-to-point communication on the Internet. Next we examine the current state of research in secure broadcasting and multicasting. As we will see, in wireless sensor networks, a great deal of the security derives from ensuring that only members of the broadcast or multicast group possess the required keys in order to decrypt the broadcast or multicast messages. Here we will address those schemes that have been specifically designed to support broadcasting and multicasting in wireless sensor networks. Traditional broadcasting and multicasting: Traditionally, multicasting and broadcasting techniques have been used to reduce the communication and management overhead of sending a single message to multiple receivers. In order to ensure that only certain users receive the multicast or broadcast, encryption techniques must be employed. In both a wired and wireless network this is done using cryptography. The problem then is one of key management. To handle this, several key management schemes have been devised: centralized group key management protocols, decentralized management protocols, and distributed management protocols. In the case of the centralized group key management protocols, a central authority is used to maintain the group. Decentralized management protocols, however, divide the task of group management amongst multiple nodes. Each node that is responsible for part of the group management is responsible for a certain subset of the nodes in the network. In the last case, distributed key management protocols, there is no single key management authority. Therefore, the entire group of nodes is responsible for key management. In order to efficiently distribute keys, one well known technique is to use a logical key tree. Such a technique falls into the centralized group key management protocols. This technique has been extended to wireless sensor networks in [19, 18]. While centralized solutions are often not ideal, in the case of wireless sensor networks a centralized solution offers some utility. Such a technique allows a more powerful base station to offload some of the computations from the less powerful sensor nodes. Secure multicasting: Di Pietro et al. describe a directed diffusion based multicast technique for use in wireless sensor networks that also takes advantage of a logical key hierarchy. In a standard logical key hierarchy a central key distribution center is responsible for disbursing the keys throughout the network. The key distribution center, therefore, is the root of the key hierarchy while individual nodes make up the leaves. The internal nodes of the key hierarchy contain keys that are used in the re-keying process. Directed diffusion is a data-centric, energy efficient dissemination technique that has been designed for use in wireless sensor networks [13]. In directed diffusion, a query is transformed into an interest (due to the data-centric nature of the network). The interest is then diffused throughout the network and the network begins collecting data based on that interest. The dissemination technique also sets up certain gradients designed to draw events toward the interest. Data collected as a result of the interest can then be sent back along the reverse path of the interest propagation [13]. Using the above mentioned directed diffusion technique; Di Pietro et al. enhance the logical key hierarchy to create a directed diffusion based logical key hierarchy. The logical key hierarchy technique provides mechanisms for nodes joining and leaving groups where the key hierarchy is used to effectively re-key all nodes within the leaving node’s hierarchy. The directed diffusion is also used in node joining and leaving. When a node declares intent to join, for example, a join “interest” is generated which travels down the gradient of “interest about interest to join”. When a node joins, a key set is generated for the new node based on keys within the key hierarchy. Secure broadcasting: Lazos and Poovendran describe a tree based key distribution scheme. They suggest a routing aware based tree where the leaf nodes are assigned keys based on all relay nodes above them. They argue that their technique, which takes advantage of routing information, is more energy efficient than routing schemes that arbitrarily arrange nodes into the routing tree. They propose a greedy routing-aware key distribution algorithm [18]. In [19], Lazos and Poovendran use a similar technique to [18], but instead use geographic location information (e.g., GPS) rather than routing information. In this case, however, nodes (with the help of the geographic location system) are grouped into clusters with the observation that nodes within a cluster will be able to reach one another with a single broadcast. Using the cluster information, a key hierarchy is constructed as in [18].

VII. CONCLUSION

In this paper, we have described the four main aspects of wireless sensor network security: obstacles, requirements, attacks, and defenses. Within each of those categories we have also sub-categorized the major topics including routing, trust, denial of service, and so on. Our aim is to provide both a general overview of the rather broad area of wireless sensor network security, and give the main citations such that further review of the relevant literature can be completed by the interested researcher. 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 a detection mechanism and making it efficient represents a great research challenge. 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] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks. IEEE Communications Magazine, 40(8):102–114, August 2002.

[2] R. Anderson and M. Kuhn. Tamper resistance - a cautionary note. In The Second USENIX Workshop on Electronic Commerce Proceedings, Oakland, California, 2006.

[3] R. Anderson and M. Kuhn. Low cost attacks on tamper resistant devices. In IWSP: International Workshop on Security Protocols, LNCS, 2007.

[4] A. R. Beresford and F. Stajano. Location Privacy in Pervasive Computing. IEEE Pervasive Computing, 2(1):46–55, 2003.

[5] D. Braginsky and D. Estrin. Rumor routing algorithm for sensor networks. In WSN '02: Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, pages 22–31, New York, NY, USA, 2005. ACM Press.

[6] D. W. Carman, P. S. Krus, and B. J. Matt. Constraints and approaches for distributed sensor network security. Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[7] J. Deng, R. Han, and S. Mishra. INSENS: intrusion-tolerant routing in wireless sensor networks. In Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado, 2002.

[8] D. Estrin, R. Govindan, J. S. Heidemann, and S. Kumar. Next century challenges: Scalable coordination in sensor networks. In Mobile Computing and Networking, pages 263–270, 1999.

[9] S. Ganeriwal and M. Srivastava. Reputation-based framework for high integrity sensor networks. In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, 2004.

[10] C. Hartung, J. Balasalle, and R. Han. Node compromise in sensor networks: The need for secure systems. Technical Report Technical Report CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.

[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, 2002, pp. 153-159.

[12] Mokowitiz, 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.

[16] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz. Secure multicast groups on ad hoc networks. In Proceedings of the 1st ACM workshop on Security of Ad hoc and Sensor Networks (SAN ’03), pages 94–102. ACM Press, 2003.

[17] O. K’omerling and M. G. Kuhn. Design principles for tamper resistant smartcard processors. In appeared in the USENIX Workshop on Smartcard Technology proceedings, Chicago, Illinois, USA, May 1999.

[18] L. Lazos and R. Poovendran. Secure broadcast in energy-aware wireless sensor networks. In IEEE International Symposium on Advances in Wireless Communications (ISWC’02), 2002.

[19] L. Lazos and R. Poovendran. Energy-aware secure multicast communication in ad-hoc networks using geographic location information. In Proceedings of IEEE International Conference on Acoustics Speech and Signal Processing, 2003.

[20] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jekerst, 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, 2010, pp. 259 – 268.

[25] Culpepper, B.J. and Tseng, H.C., “Sinkhole intrusion indicators in DSR MANETs”, Proc. First International Conference on Broad band network, 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 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.

[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 Efficient Routing 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 Enabling Technologies: 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, 2009, pp. 162 – 175.

AUTHOR BIOGRAPHY

Pulkit Berwal : B.tech, M.tech.
From University institute of engineering and technology, M.D University, Rohtak.