International Journal of Scientific Research & Engineering Trends
Volume 4, Issue 3, May-June-2018, ISSN (Online): 2395-566X

Analysing Various Security Attacks in Remote Sensor Networks

Er. Himanshi Vashisht
CSE Department Haryana
Engineering college Jagadhri
Haryana, India

Associate Professor Sanjay Bharadwaj
D.A.V College for Girls
Yamunanagar, Haryana, India

Sushma Sharma
D.A.V College for girls
Yamunanagar, Haryana, India

***Abstract* – A remote sensor networks is a recent advancement of technology of computer networks and electronics. Its sensing technology in combination with its processing power and wireless communication makes it productive for its abundant exploitation in the near future. A remote sensor arrangement generally, contains sensors, actuators, memory, a processor. The nodes in this network are not connected to a central node, and are self-managing. They are not connected to a specific network topology, practise multi-way routing, preserving the integrity and confidentiality of data, and are robust making them highly applicable for military applications. With development in such applications, security of data has become a crutial need keeping in mind that the end goal is to ensure that the touchy and confidential informationis also included. These networks are prone large number of disastrous attack or hacks such as Sybil, Wormhole, Sinkhole, etc. that threaten data flow or may have a motive to disrupt the entire network. The assault becomes even more viable when the attacker incorporates itself on the way of information flow. In this context, we analysis security aspects of the remote sensor networks like requirements, classificati ons, and type of attacks etc., in this survey paper.**

***Keywords* – Blackhole attack, DoS attack, Jamming, Remote Sensor Network**.

I. INTRODUCTION

Remote Sensor Networks (RSN) are rising as a "Modern Day Technology" which is drawing a lot of researchers attention and consideration. They are emerging as an important tier in the IT and also active research in hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors[1].

The current advances in minimal effort, low power gadget and radio advances have strengthened the development of RSN. It has a wide range of applications including measuring microclimates on farms, monitoring traffic, steer traffic away from jams, accidents alert emergency services, detecting human presence in homes and offices etc. [4]. With the variety in applications there may occur variety of attacks on the RSN.

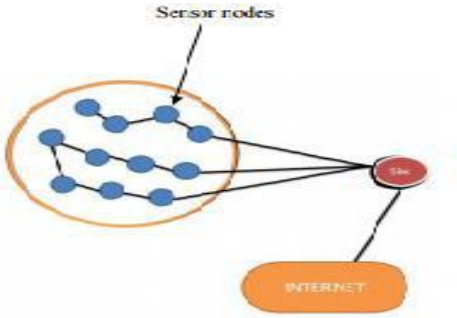

Figure 1- Simple architecture of a RSN.

A remote sensor network is a group of self- organized sensor nodes that combines sensing, computation and communication in a single small sensor node. [3]. A sensor node consists of a sensing unit that is responsible for sensing the information and sending that information to nearby or neighbour nodes.

The information that is sensed by the sensor is sent to the Processing unit that processes the sensed information from the sensors. A Communication Unit is responsible for communicating with the neighboring nodes using the radio signals. Power Unit is responsible for supplying the battery power to the nodes. The nodes in the WSN are battery operated. A RSN also has gateway sensor nodes transfers the data from the sink node to the internet. The remote users can access the contents of the Internet. The sensors collects the data like pressure, temperature, light, motion, sound etc and processes this data using its microcontrollers and microprocessors.

The main goal of the applications is achieved when all the sensor nodes work collectively. Sensor nodes sense and process the data from the surrounding environment and route it to the sink or Base Station either through single hop or multi-hop technique depending on the distance between the sensor nodes and sink. This data is in turn transmitted to the user via other secondary links such as internet.[5]. These nodes lack in energy and memory and therefore various routing protocols needs to be devised that compensate its deficiencies and also

maximize the network lifetime. Today's sensors can monitor temperature, pressure, humidity, soil, 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.[1]

II. CHARACTERISTICS OF RSN

[1].Communication medium: Nodes in WSN utilize wireless medium for communication, for example, radio waves or infrared waves.

[2]. Hardware Constraints: WSN nodes use battery for working. Life of these nodes relies upon the exhaustion of the batteries. WSN is limited as far as memory is concerned.[3].

[3]. Application Dependent: Wireless Sensor Networks are application needy as they are intended for ongoing accumulation and examination of data. It is highly dependent on the application such as from military, environmental and health sector. The nodes are deployed randomly depending on their use.[4].

[4].Distributed Processing: In Wireless Sensor Networks processing is done by each node, so a unified instrument ought to be used to total the data. This may require a large number of sensor node. These nodes are distributed uniformly or randomly. Each node can collect, sort, process, aggregate and send the data to the sink. Therefore, the distributed processing provides the robustness of the system.[5].

[5]. Prone to attacks: As Wireless Sensor Networks are generally conveyed in cruel natural conditions where securing the networking is genuinely troublesome, so these networks are inclined to attacks.[1].

[6]. Multi-hop Routing: Sensor nodes communicate with each other to transmit information to sink. They utilize the immediate transmission or multi-hop transmission to speak with the base station.[5].

[7]. Communication paradigm: There is a predefined view of communication as all the sensor nodes sense data in various situations according to the query of the sink node. It may also need to send the data back and forth from sink to node.[5].

III. SECURITY ISSUES IN RSN

The current advances in minimal effort, low powered gadgets, and radio service advances have strengthened the development of RSN systems with the wide range of applications including the front line reconnaissance, military observing framework, home mechanization, ecological checking, human services checking and some more.

RSN provides a large number of applicaions particularly that comprises of expansive number of ease, low power, asset obliged,imparting utilizing the remote medium and are th ickly and arbitrarily sent with no fixed topology in remote and threatening areas.[4]. The sensor nodes are normally battery fueled and have extremely constrained assets as far as vitality, stockpiling, and handling abilities are concerned.[3]. To detect, locally process the data and convey it to the sink are three key undertakings of a sensor hub. Other than giving the unlimited openings, RSN gives security challenges as a result of delicate information included, constrained battery and memory assets and unattended conditions.[1].

RSN are powerless against security attacks which can occur either inside or outside the system. Outside attacks are not exceptionally successful and do not make much harm to the systems since they do not have the entrance to the system data. However, the inside attacks are extremely powerful and can disturb the working of the entire system as enemy is a piece of system and approaches the data of the system. This makes it hard to identify the enemy which utilizes various security components, approval and confirmation as the enemy is true blue individual from the system.

IV. ATTACKS IN RSN

The basic categories of attacks on RSN's data privacy are eavesdropping, disruption and hijacking.

1. **Eavesdropping-** It is used to know the output of sensor nodes. There are mainly two ways to know about this output data by sending queries to sensor nodes or aggregation points or attacks sensor nodes. The former approach is called passive eavesdropper and later approach is called active eavesdropper. The location of eavesdropper plays major role in getting information. Confidentially and authentication in RSN are affected due to eavesdropping.
2. **Disruption-** It mainly influences the output of the network. It injects messages, corrupts data or changes values in order to make the data corrupted, useless and incomplete. Physical disruption renders the sensor readings by directly manipulating the environment.
3. **Hijacking-** It usually takes control over sensor node in network. Eavesdropping and disruption becomes easy by hijacking the main sensor nodes.

Other critical attacks in RSN are as follows-

1. **Denial of Service attack-** Denial of Service or DoS [7],[8] happens when there is an unintentional failure of sensor nodes caused by some malicious action. This makes them inaccessible to the user. Extra and unnecessary packets are sent to the victim node, preventing legitimate network users from accessing services and resources.

There are several types of DoS attacks in different layers that might be performed. At physical layer the DoS attacks could be jamming and tampering. In link layer, collision, exhaustion, unfairness can be some usual attacks. At network layer, neglect and greed, homing, misdirection, blackholes are carried out. In

transport layer malicious flooding and resynchronizations can occur.

2. **Sybil attack-** In a Sybil attack [9],[10] the attacker misleads other nodes by projecting a wrong or duplicate ID of the users. In this attack a node may represent multiple identities to the rest of the nodes. This attack can be performed by creating a fake arbitrary node or by stealing an identity from a legitimate node, leading to a corruption of the routing protocols.

   These attacks can cause threat to geographical routing protocols, since they require the exchange of coordinates for efficient packet routing. In ideal conditions, usually a node sends a set of coordinates, but under a Sybil attack, it occurs to be present in many places in one time. In the latest network environment, many alien nodes can appear in disguise using various identities and act as original nodes.
3. **Black hole attack-** Black-hole attacks [11],[12],[13] also called packet drop attacks or sinkhole attacks, are one type of denial-of-service attack that is caused by an external element on a sensor nodes in a network. The adversary reprogrammed the nodes such that they do not transmit the data packets.

   These nodes called black hole nodes and the region which holds such nodes is known as the black hole region. As a result of this attack any information that enters in the black hole region is captured and does not reach the base stations. The network performance parameters are affected due to this attack causing throughput to decrease significantly and increasing end-to-end delay.
4. **Hello Flood attack-** In a RSN some routing protocols requires the sensor nodes to broadcast hello messages to announce themselves to their neighbour nodes. These protocols may assume that receiving this hello message means that the sender is within radio range and is therefore a neighbour.

   An adversary may use a high powered transmitter to track a large area of nodes believing that they are neighbours of that transmitting node. For example, an adversary can advertise a very high quality route to the sink, which can lead to a large number of nodes using that route. But if these nodes which are sufficiently far away from the adversary this can cause sending the packets into oblivion. Hence, causing the network to be left in a state of confusion. Protocols which depend on localized information exchange between neighbouring nodes for topology maintenance or flow control are affected due to this attack.[14],[15],[16],[17].
5. **Worm hole attack-** Wormhole attack [18],[19],[20],[21] is a critical attack in which the attacker records the packets or bits at one location in the network and tunnels them to some other location. Insertion of two nodes is required to accomplish this attack. These two nodes are interconnected by a strong connection. Any routing protocol used in RSN generally uses number of hops to calculate the shortest path. But in this attack, the two malicious nodes can achieve a distant location within a single jump. This possibility can be misleading for the other nodes, thus, forming a wormhole. The victim nodes will try to use the fastest route which would be the one formed by the wormhole. As a consequent, causing the information to be easily retrieved by the attacker.
6. **Byzantine attack-** In byzantine attack[22],[23] the victim nodes drops packets continuously and behave like normal node. When these packets are continuously dropping they create a collision in the network causing performance degradation. Byzantines intend to deteriorate the performance of the network by suitably modifying their decisions. As the end goal of the attacker is to assault the system a halfway hub is traded off.

   The different steering circles and dropping parcels interfere with the system or creates such awful conditions that makes it hard to give directions to the administrations inside this system.
7. **Jamming-** Jamming attacks[24],[25],[26],[27] aim to interfere in RSN by emitting jamming signals thus, affecting the data transmission and reducing performance. The resources overutilization affects battery life, memory, etc. There are different types of jamming techniques that try to intentionally interfere with the communication between two nodes like Constant jammer that continually emits a radio signal.

   Deceptive jammer is another type of jammer. It constantly injects regular packets without any gap between transmissions rather than randomly sending bits. A Random jammer instead of continuously sending out a radio signal, alternates between sleeping and jamming. after jamming for some time, it turns off its radio and enters into sleeping mode. During its jamming phase, it can behave like either a constant jammer or a deceptive jammer. This model takes energy conservation into consideration. Reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. One advantage of a reactive jammer is that it is harder to detect.
8. **Man-in-the-middle-** The man-in-the-middle attack [28], [29] is a form of active eavesdropping in which the attacker makes independent connections with the two or more victim nodes and intercepts message transmissions between them. It makes them believe that they are talking directly to each other over a private connection which is not the actual case as the whole communication process is manipulated by the attacker. The attacker can also inject new messages [30]. This type of attack is able

to steal the information no matter what type of security mechanism is implemented.

V.CONCLUSIONS AND FUTURE WORK

As WSNs are being used more frequently and more rapidly, the need for their security becomes even more apparent. Although, the nature and design of RSN sensor nodes makes energy, processing capability limited, still there usage and requirement is evident. In this article, we have surveyed the some popular security issues and attacks in RSNs. Security in RSNs are becoming more apparent thus preventing the network from attacks has become the prime goal for researchers. In the absence of proper security the RSNs are vulnerable to various attacks like sinkhole, Sybil, black hole, jamming etc. causing confidentiality, integrity, authentication and data freshness to be stake. Security measures are highly desirable and are needed in many applications. In future work we will explore the existing Security protocols and techniques & will propose a novel technique to have a much secure RSN.

REFERENCES

[1]. T. Azzabi, H. Farhat, N. Sahli ., "A Survey on Wireless Sensor Networks Security Issues and Military Specificities Security of Sensitive Systems" International Conference on Advanced Systems and Electric Technologies

[2]. I. Ahmad, K. Shah, S. Ullah., "Military Applications using Wireless Sensor Networks: A survey". International Journal of Engineering Science and Computing, Volume 6 Issue No. 6, June 2016.

[3]. M. Anand, E. Cronin, M. Sherr, M. Blaze, Z. Ives, and I. Lee, "Sensor Network Security: More Interesting Than You Think", In Proc. of the 1st USENIX HotSec, 2006.

[4]. D.P. Agrawal, "Embedded Sensor Systems" Springer Nature Singapore Pte Ltd. 2017 DOI 10.1007/978-981-10- 3038-3_2.

[5]. A. Rani, S. Kumar, "A Survey of security in Wireless Sensor Networks" 3rd IEEE International Conference on "Computational Intelligence and Communication Technology" (IEEE-CICT 2017).

[6]. R. Dubey, V. Jain, R.S. Thakur, S.D. Choubey., "Attacks in WSN", International Journal of Scientific & Engineering Research, Volume 3, Issue 3, March-2012 ISSN 2229-5518.

[7]. 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.

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

[9]. S. Sharmila and G. Umamaheswari, "Detection of sybil attack in mobile wireless sensor networks," International Journal of Engineering Science&Advanced Technology, vol. 2, pp. 256–262, 2012.

[10]. R. Amuthavalli, Dr. R. S. Bhuvaneswaran, "Detection and Prevention of Sybil Attack In Wireless Sensor Network Employing Random Password Comparison Method ", Issue September 2014(JTAIT).

[11]. V. Taylor and D. Fokum, "Securing wireless sensor networks from denial-of-service attacks using artificial intelligence and the clips expert system tool," in Southeastcon, 2013 Proceedings of IEEE, 2013, pp. 1–6.

[12]. Afrand, Agah and Sajal, K. 2007.Preventing DoS Attacks in Wireless Sensor Networks: A Repeated Game Theory Approach. International Journal of Network Security, 5(2):145–153.

[13]. B. K. Mishra, "Security against Black Hole Attack in Wireless sensor Network-A Review,2014 Fourth International Conference on Communication Systems and Network Technologies. pp.615-620, IEEE 2014.

[14]. S. Magotra, K. Kumar," Detection of HELLO flood attack on LEACH protocol", IEEE 2014.

[15]. Chris Karlof, David Wagner,(2003) Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures, IEEE.

[16]. Dr. Moh. Osama K., (2007),Hello flood counter measure for wireless sensor network, International Journal of Computer Science and Security, volume (2) issue (3).

[17]. A Hamid, S Hong, (2006) Defense against Lap-top Class Attacker in Wireless Sensor Network, ICACT.

[18]. Kia Xiang, Shyaam Sundhar Rajamadam,Srinivasan, Manny Rivera,Jiang Li, Xiuzhen Cheng, "Attacks and Countermeasures in Sensor Networks: A Survey", pp 1-28, Springer, 2005.

[19]. G. Padmavathi, Mrs. D. Shanmugapriya, "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security Vol. 4, No. 1 & 2, 2009.

[20]. Dhara Buch, Devesh Jinwala, "Detection of Wormhole Attacks in Wireless Sensor Networks", IEEE Conference on Advances in Recent Technologies in Communication and Computing, pp 7-14, 2011.

[21]. Khin Sandar Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 24, 2008.

[22]. Jen-Yeu Chen and Yi-Ying Tseng, "Distributed Intrusion Detection of Byzantine Attacks in Wireless Networks with Random Linear Network Coding", IEEE, 2013 .

[23]. Stefano Marano, Vincenzo Matta, and Lang Tong, "Distributed Detection in the Presence of Byzantine Attacks", IEEE TRANSACTIONS ON SIGNAL PROCESSING, VOL. 57, NO. 1, JAN 2009 .

[24]. A.D. Wood, J.A. Stankovic and S.H. Son "JAM: A Jammed-Area Mapping Service for Sensor Networks", In Real-Time Systems Symposium (RTSS), Cancun, Mexico, 2003.

[25]. Poisel Richard, "Modern communications jamming principles and techniques".

[26]. F.C.M. Lau and C.K. Tse, " Study of Anti-Jamming Capabilities of Chaotic Digital Communication Systems," Proceedings, 2002 International Symposium on Nonlinear Theory and Its Applications, (NOLTA'2002), October 2002, Xian, China, pp.65-68.

[27]. [27] Wenyuan Xu et. AI. "Jamming Sensor Network: Attack And Defence Strategies" .

[28]. [28] Z. Chen, S. Guo, K. Zheng, and H. Li, \Research on manin-the-middle denial of service attack in sip voip," Networks Security, Wireless Communications and Trusted Computing, NSWCTC, vol. 2, pp. 263{266, Apr. 2009.

[29]. G. N. Nayak and S. G. Samaddar, \Di_erent avours of manin-the-middle attack, consequences and feasible solutions," Computer Science and Information Technology (ICCSIT), vol. 5, pp. 491{495, July 2010.

[30]. Manishaben Jaiswal, "Computer Viruses: Principles Of Exertion, Occurrence And Awareness", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Volume.5, Issue 4, pp.648-651, December 2017.

AUTHOR PROFILE

Himanshi Vashisht is a student of M.Tech in Computer Science Engineering, HEC, Jagadhri, Haryna INDIA. She was involved in many Java application based project during her B.Tech. Her research area includes Wireless Sensor Networks.