Journal for Research | Volume 02 | Issue 07 | September 2016
ISSN: 2395-7549

Security Threats in Sensor Network in IoT: A Survey

Anand singh
M. Tech. Student
Department of Electronics & Communication Engineering
Apex Group of Institutions, Karnal, Haryana, India

Anupma goyal
Lecturer
Department of Electronics & Communication Engineering
Apex Group of Institutions, Karnal, Haryana, India

Abstract

In recent years, wireless sensor network (WSN) is used in several application areas resembling observance, tracking, and dominant in IoTs. for several applications of WSN, security is a crucial demand. However, security solutions in WSN disagree from ancient networks because of resource limitation and process constraints. This paper analyzes security solutions: TinySec, IEEE 802.15.4, SPINS, MiniSEC, LSec, LLSP, LISA, and LISP in WSN. This paper additionally presents characteristics, security needs, attacks, cryptography algorithms, and operation modes. This paper is taken into account to be helpful for security designers in WSNs.

Keywords: IoT, Sensor Network

I. INTRODUCTION

Typically, WSNs contain an outsized range of detector nodes, that square measure densely and haphazardly deployed within the field underneath study as shown in figure one. every of those scattered detector nodesh because the capabilities to gather information and route information back to a set purpose referred to as a Sink. Information square measure forwarded to the Sink through a multihop wireless design as shown in figure1. Once the collected information reaches the sink, it's to route them to the task manager, wherever the suitable choices is created. The sink might communicate with the task manager node via net or satellite. the aim of deploying a WSN is to report relevant information for process that permits right higher cognitive process at the proper moment. There square measure 3 styles of reporting: event-driven, on-demand and continuous observance. within the event-driven reportage, the detector network is ready-made to sight the prevalence of a pre-specified variety of event at intervals the detector field. Once this event happens, the reportage task is initiated and therefore the connected info is forwarded to the Sink. Therefore communication is triggered by the event prevalence and solely nodes at intervals the event space become sources of communication. The foremost noted detection primarily based applications are: hearth, food detection and alarms. within the on-demand reportage, communication is initiated by the Sink, and detector nodes finish their information in response to a definite request. The vital corresponding application is a listing system. one among the key options of a WSN is its multihop distributed operations, that add a lot of quality in terms of security attack detection and hindrance. during a multihop distributed atmosphere, it's terribly troublesome to find attackers or malicious nodes. several security attack detection and hindrance mechanisms square measure designed for WSNs; but most of the present solutions square measure capable of handling solely a couple of security attacks. Let's say, most secure routing protocols square measure designed to counter few security attacks.

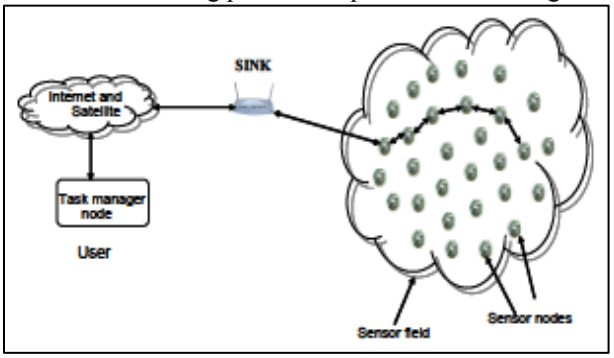

Fig. 1: WSN design

Similarly new media access mechanisms square measure designed to handle hidden-node drawback or stinginess. cryptography mechanisms square measure designed to guard information against passive attacks. Hence, one will say that there's a requirement to style mechanisms that square measure capable enough of sleuthing and preventing multiple security attacks in WSNs. Associate in Nursing Intrusion Detection System (IDS) is one potential resolution to that. Associate in Nursing intrusion is essentially any variety of unlawful activity that is meted out by attackers to damage network resources or detector nodes.

Associate in Nursing IDS may be a mechanism to sight such unlawful or malicious activities. the first functions of IDS square measure to observe users' activities and network behaviour at totally different layers. one good defence is neither possible nor potential in wireless networks, as there continuously exist some subject area weaknesses, software system bugs, or style flaws which can be compromised by intruders. the simplest observe to secure wireless networks is to implement multiline of security mechanisms; that's why IDS is a lot of essential in wireless networks. it's viewed as a passive defense, because it isn't supposed to stop attacks; instead it alerts network directors regarding potential attacks well in time to prevent or scale back the impact of the attack. The accuracy of intrusion detection is mostly measured in terms of false positives (false alarms)and false negatives (attacks not detected), wherever the IDSs conceive to minimize each these terms. There square measure 2 vital categories of IDSs. One is thought as signature-based IDS, wherever the signatures of various security attacks square measure maintained during a info. this type of IDS is effective against well-known security attacks. However, new attacks square measure troublesome to be detected as their signatures wouldn't be gift within the info. The second kind is anomaly-based IDS. this type is effective to sight new attacks; but it typically misses to sight well-known security attacks. the explanation is that anomaly-based IDSs don't maintain any info, however they incessantly monitor traffic patterns or system activities.IDS will operate in several modes, let's say, standalone operation and cooperative cluster primarily based operation. A standalone IDS operates on each node to sight unwanted activities. Cooperative cluster largely|primarily based} IDS square measure mostly distributed in nature within which each node monitors its neighbours and encompassing nodes activities and operation; just in case of any malicious activity detection, the cluster head is knowing. loosely, IDS has 3 main parts as:

- Observance part is employed for native events observance furthermore as neighbours observance. This part largely monitors traffic patterns, internal events, and resource utilization.
- Analysis and detection module is that the main part that is predicated on modelling rule. Network operations, behaviour, and activities square measure analyzed, and choices square measure created to declare them as malicious or not.
- Alarm part may be a response generating part, that generates Associate in Nursing fearsome case of detection of Associate in Nursing intrusion.

II. PREVIOUS WORK

Intrusion detection system (IDS) may be a system capable of sleuthing a variety of intrusions and attacks. Dennig in [10] outlined Associate in Nursing intrusion detection model. intoxicating et al. in [11] designed a system observance a neighborhood network and capturing info regarding information packet transmission. The design of the IDS consisted of information sampling and preprocessing part and a classifier system. the info provided to the classifier system were following: packet size price, timestamp price and LAN source-destination ordered combine. The rule-based system might be run in either learning method or during a call method. A credit assignment rule was wont to assign a credit to the foundations and a genetic rule was wont to delete the foundations or to come up with new ones. Since that point, several intrusion detection systems are developed for wired and additionally wireless networks. Zhang and Lee in [12] delineated vulnerabilities of normal unexpected wireless networks and revealed their work on intrusion detection and response mechanism appropriate for normal unexpected wireless networks. They compared the normal unexpected wireless networks with mounted wired networks and noted that the ad-hoc wireless networks didn't have such concentration traffic purpose like routers, switches or gateways because the wired networks had. Hence, the sole potential audit trace was restricted to radio traffic and IDS techniques had to be supported some partial and localized info. They recommended that the IDSs appropriate for normal unexpected wireless networks ought to be distributed and cooperative. Pires et al. in [13] thought of an answer for malicious node detection in WSNs supported the received signal strength.

Silva et al. in [14] projected Associate in Nursing IDS fitting the strain and needs of WSNs. They claimed that the designer of Associate in Nursing IDS ought to 1) choose from the out there set of rules those who is wont to monitor the required features; 2) compare the knowledge needed by the chosen rules with the knowledge out there within the target WSN to pick final set of rules; and 3) set the parameters of the chosen rules with the values of the look definitions. we tend to believe that our projected IDS framework can considerably facilitate the network operators to follow this recommended method.

A. Classification

Techniques employed in intrusion detection systems are classified into 2 following classes:

- Signature (misuse) detection. Techniques supported signature detection square measure wont to determine glorious intrusions. Let's say, they will analyze sniffed packets to search out whether or not they square measure malicious or not. The advantage is that the techniques supported signature sightion will effectively and accurately detect glorious attacks. The disadvantage is that they can't acknowledge novel attacks with unknown signatures. • Anomaly detection. Techniques supported anomaly detection ought to be ready to acknowledge unknown attacks as a result of the traffic patterns is compared with "training sets" characterizing traditional behavior. If the pattern deviates considerably, Associate in nursing intrusion is according. The advantage is that the techniques supported anomaly sightion don't need any previous data of the attacks and might detect novel intrusions. The disadvantage is that they will doubtless cause high quantity of false negatives or positives and can't describe what reasonably attack occurred. Providing a reliable coaching set may additionally be problematic.

B. Parts and Design

Silva et al. in [14] recommended to divide their rule for Associate in Nursing intrusion detection system into 3 phases: 1) information acquisition, wherever packets square measure collected during a promiscuous mode and filtered before storage for additional analysis; 2) rule application, wherever rules square measure applied on the hold on data; and 3) intrusion detection, wherever the range of failures generated within the previous section is compared to the amount of often expected number of failures to think about whether or not Associate in Nursing intrusion occurred. Roman et al. in [15] noted that it's impractical to possess an energetic intrusion detection agent in each node of a WSN thanks to restricted battery capability and projected a general design for WSNs. They divided intrusion detection agents into 2 following classes:

- Native agents monitor the activities performed on the node itself and on the sent or received packets. The agent solely manages its own communication thus the overhead is low.
- International agents monitor the communication of its neighbors and analyze the content of the overheard packets. they will even be referred to as watchdogs. solely bound nodes during a WSN ought to sometimes move agents at a time thus on conserve the energy and to prolong the general network time period. each node ought to store info regarding the safety (information regarding alerts and suspicious nodes) and therefore the atmosphere (list of the neighbors). In its internal alert info, the intrusion detection agent ought to store the safety info generated by itself (containing time of creation, classification and supply of the alert) [15].

C. Techniques

Pires et al. in [13] thought of detection of hi flood and hollow attacks in WSNs if a sign strength of a neighbor received by the IDS was incompatible with the assumed geographical positions of that neighbor. The detection was supported comparison of the received signal strengths with the expected values supported geographical info and therefore the predefined transceiver specification. If some node was suspicious, the node that detected it broadcasted {the info|the knowledge|the data} victimization suspicious node information dissemination protocol. However, the localization of the malicious nodes was left for the longer term work. timberland et al. in [14] outlined rules that may be used for intrusion detection in WSNs. Interval rule is wont to live the time between the reception of 2 consecutive packets. If it's large, the interloper may not send information generated by a tampered node. If it's too little, the interloper might increment the packet causation rate so as to extend battery depletion of its neighbors. Retransmission rule is wont to ascertain whether or not packets alleged to be forwarded by a neighbor were forwarded or to not sight selective forwarding or blackhole attack. Integrity rule is wont to sight unauthorized modifications of the packets. Delay rule is wont to live whether or not Associate in Nursing intermediate node on the trail delayed packets or not. Repetition rule is wont to live whether or not a retransmission of constant packet exceeded predefined limit to sight denial of service or jam. Radio transmission vary is wont to live whether or not all overheard packets were originated from one among the $64000 neighbors to sight hollow and hi flood attack. Jamming rule is wont to live the amount of collisions related to a packet sent by the observance node to sight jamming. Roman et al. in [15] projected that native agents ought to monitor attacks against logical and physical safety of the node (whether they're manipulated), measurements of the sensors (whether they follow bound patterns) and packets directly addressed to its node (whether they follow applied protocols). Additionally, they ought to manufacture Associate in Nursing alarm if a brand new neighbour is overheard or if a sign is crowded. International agents ought to monitor primarily packet dropping and modification by analyzing communication of their neighbors. they will additionally behave as spontaneous watchdogs. If they hear a packet not addressed to them and therefore the receiver is their neighbor, they monitor the forwarding of that packet with chance 1/n, wherever n is that the range of nodes that may monitor constant forwarding of constant packet as well.

III. CONCLUSION

The network operator considers the vulnerabilities associate specifies the attacks exploitable by an assailant so as to compromise the network. In my work, i will be able to specialise in selective forwarding, delay and modification attacks, wherever the changed packets square measure monitored and therefore storage overhead is generated. The detection techniques is optimized to get decent accuracy at the value of cheap consumption of the resources. Another (if time and alternative resources permit) thought of attack would be jam, wherever parameters resembling carrier sensing time1 or range of retransmissions square measure monitored and corresponding thresholds can be optimized. Last however not least, another doubtless thought of attack would be the Sybil attack, wherever the attacker's node changes its identity. The framework is going to be long to hide alternative techniques and to optimize them.

REFERENCES

[1] Murat Dener, "Security Analysis in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, vol. 2014
[2] Kahina CHELLI," Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", Proceedings of the World Congress on Engineering 2015 Vol I WCE 2015, July 1 - 3, 2015, London, U.K
[3] Peng Zhou; Siwei Jiang; Irissappane, A.; Jie Zhang; Jianying Zhou; Teo, J.C.M., "Toward Energy-Efficient Trust System Through Watchdog Optimization for WSNs," in Information Forensics and Security, IEEE Transactions on , vol.10, no.3, pp.613-625, March 2015

[4] Ching-Tsung Hsueh; Chih-Yu Wen; Yen-Chieh Ouyang, "A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks," in Sensors Journal, IEEE , vol.15, no.6, pp.3590-3602, June 2015
[5] Martin Stehl´ık, Adam Saleh, Andriy Stetsko and Vashek Matya´s," Multi-Objective Optimization of Intrusion Detection Systems for Wireless Sensor Networks", Advances In Artificial Life, ECAL 2013
[6] Raza, F.; Bashir, S.; Tauseef, K.; Shah, S.I., "Optimizing nodes proportion for intrusion detection in uniform and Gaussian distributed heterogeneous WSN," in Applied Sciences and Technology (IBCAST), 2015 12th International Bhurban Conference on , vol., no., pp.623-628, 13-17 Jan. 2015
[7] Yun Wang; Weihuang Fu; Agrawal, D.P., "Gaussian versus Uniform Distribution for Intrusion Detection in Wireless Sensor Networks," in Parallel and Distributed Systems, IEEE Transactions on , vol.24, no.2, pp.342-355, Feb. 2013
[8] Nabil Ali Alrajeh, S. Khan, and Bilal Shams, "Intrusion Detection Systems in Wireless Sensor Networks: A Review," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 167575, 7 pages, 2013
[9] Quazi Mamun, Rafiqul Islam, and Mohammed Kaosar," Anomaly Detection in Wireless Sensor Network" Journal Of Networks, Vol. 9, No. 11, November 2014
[10] D. E. Denning. An intrusion-detection model. IEEE Transactions on Software Engineering, (2):222–232, 1987
[11] R. Heady, G. Lugar, M. Servilla, and A. Maccabe. The architecture of a network level intrusion detection system. Technical report, University of New Mexico, Albuquerque, NM, August 1990
[12] Y. Zhang and W. Lee. Intrusion detection in wireless ad-hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking, MobiCom '00, pages 275–283, New York, NY, USA, 2000. ACM
[13] W. R. Pires Jr, T. H. de Paula Figueiredo, H. C. Wong, and A. A. F. Loureiro. Malicious node detection in wireless sensor networks. In Parallel and Distributed Processing Symposium, 2004. 18th International Proceedings, page 24, 2004.
[14] A. P. R. da Silva, M. H. T. Martins, B. P. S. Rocha, A. A. F. Loureiro, L. B. uiz, and H. C. Wong. Decentralized intrusion detection in wireless sensor networks. In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, pages 16–23, 2005.
[15] R. Roman, J. Zhou, and J. Lopez. Applying intrusion detection systems to wireless sensor networks. In IEEE Consumer Communications & Networking Conference (CCNC 2006), pages 640–644, Las Vegas (USA), January 2006