Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Introduction of Wireless Sensor Network Attacks and Its Analysis, Its Characterstics, Weakness, Security Issues and Fractal Propagation

[1]Er. Aman Dhiman, [2]Er. Rupinder Kaur, [3]Er. Manjit Thapa, [4]Er. Bhubneshwar Sharma
[1]M.Tech Student, [4]Assistant Professor,
[1, 4] Department of Electronics and Communication Engineering, Arni University, H.P., India
[2, 3] Assistant Professor, Department of Computer Science and Engineering, Eternal University, H.P., India

Abstract: ***Targeting the base station is also the most efficient use of an attacker's resources, since energy, time, and effort need be expended to destroy only a small number of base stations rather than to destroy every sensor node in the network. Given that the number of base stations in a WSN is relatively small, the pronounced data traffic pattern.A security mechanism based on signal strength and geo-graphical information is for detecting malicious nodes that launching hello flood and wormhole attack. The detection rate of the solution depends on different parameters such as network density, transmission power multiplier of the malicious node, message checking probability etc. Besides, the same kind of attacks may be present in multiple layers, althoughthey use different techniques. For instance, denial of services (DoS) attacks exist in physical layer, MAC layer, and network layer ,Sybil attacks exist in both MAC layer and network layer For each kind of such attacks, since their fundamentals are the same, our discussion on their characteristics is usually more detailed in one layer than in others***

Keywords:-MAC, WSN, DOS.

I. INTRODUCTION

As soon as the network identifies a defect or detects incorrect data forwarding, it uses a systematic rerouting to avoid attacks. Those protocols which use serial number, when forwarding a package, can identify fake messages. Thus they are able to identify the messages sent by black hole node. It is clear that we must discard many preconceptions about network security: sensor networks differ from other distributed systems in important ways.The survey on wireless sensor network security is vast, with various attacks and counter measures by various researchers. Countermeasures for these attacks exist at different sensor network levels and they are aimed at giving protection to the data during different levels of the receiving, processing and distribution process. Various methodologies are for ensuring security in WSNs have been seen and summarized both at the higher level as well as at the low levels. In WSNs, the issue of having security and design of routing algorithms is very important to study the design properties like connectivity, node coverage and fault tolerance. Protocols resistant against different formations can also reduce the effect of this attack. These protocols do not confine themselves to the nodes' position in choosing a node as the next node to send data towards the sink and the nodes' remaining energy is efficient in algorithm selection. The resource-starved nature of sensor networks poses great challenges for security.

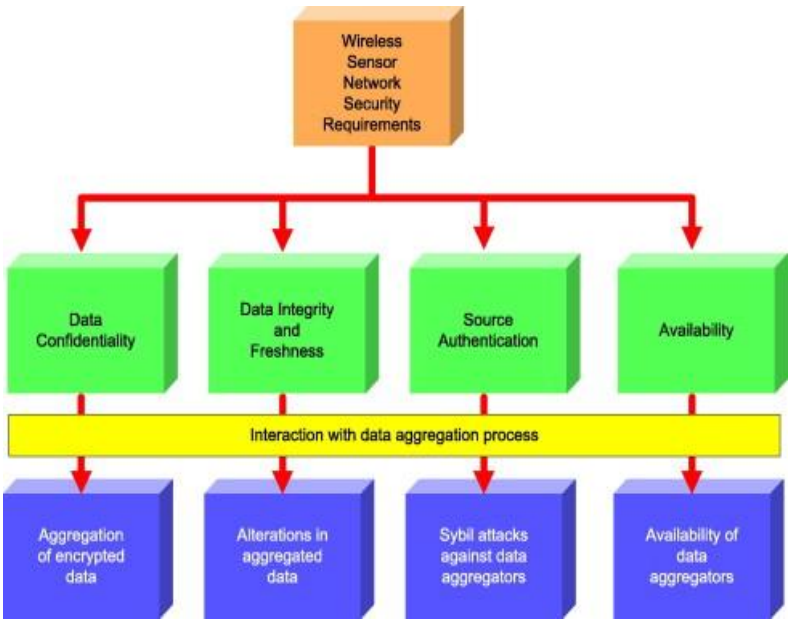

Figure1- Wireless sensor networks security requirements

These devices have very little computational power: public-key cryptography is so expensive as to be unusable, and even fast symmetric-key ciphers must be used sparingly also, communication bandwidth is extremely dear: each bit transmitted consumes about as much power, and as a consequence, any message expansion caused by security mechanisms comes at significant cost. Various Wireless sensor networks security requirements are shown in figure1.Power is the scarcest resource of all: each milliamp consumed is one milliamp closer to death, and as a result, nearly every aspect of sensor networks must be designed with power in mind. Although some solutions have already been proposed, there is no single solution to protect against every threat. In our paper we mainly focus on the security threats in WSN.

There're many security mechanisms which are used in „layer-by-layer" basis as a security tool. Recently researchers are going for integrated system for security mechanism instead of concentrating on different layers independently. Through this paper we'vetried to present the most common security threats in various layers [1]. The attack models for digital signature can be classified into known-message, chosen-message, and key- only attacks. In the known message attack, the attacker knows a list of messages previously signed by the victim. In the chosen-message attack, the attacker can choose a specific message that it wants the victim to sign.

II. ATTACKING WIRELESS SENSOR NETWORKS

Sensor networks are a promising new technology to enable economically viable solutions to a variety of applications, for example pollution sensing, structural integrity monitoring, and traffic monitoring [2]. A large subset of sensor network applications requires security, especially if the sensor network protects or monitors critical infrastructures. The Attacking Architecture is shown in figure2 .Security in sensor networks is complicated by the broadcast nature of the wireless communication and the lack of tamper-resistant hardware (to keep per-node costs low). In addition, sensor nodes have limited storage and computational resources, rendering public key cryptography impractical.

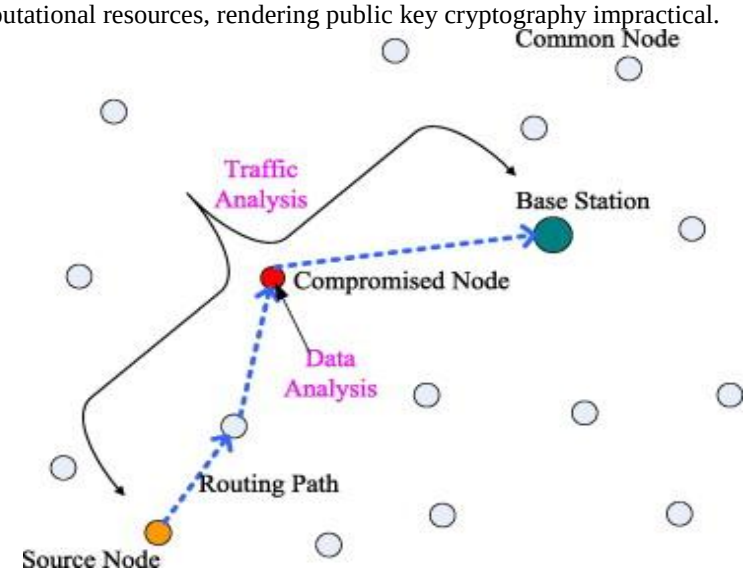

Figure2.Attacking Architecture.

By ensuring that all traffic in the targeted area flows through a compromised node, an adversary can selectively suppress or modify packets originating from any node in the area. It should be noted that the reason sensor networks are particularly susceptible to sinkhole attacks is due to their specialized communication pattern. Since all packets share the same ultimate destination (in networks with only one base station), to influence a potentially large number of nodes a compromised node needs only to provide a single high quality route to the base station.We can identify the purpose and capabilities of the attackers; also, the goal and effects of the link layer attacks on WSNs are introduced [3]. Due to unsafe and unprotected nature of communication channel, untrusted and broadcast transmission media, deployment in hostile environments, automated nature and limited resources.

III. ANALYSIS WITH SRP METHOD

Due to either the real or imagined high quality route throughthe compromised node, it is likely each neighboring node ofthe adversary will forward packets destined for a base stationthrough the adversary, and also propagate the attractiveness ofthe route to its neighbors. Effectively, the adversary creates alarge "sphere of influence", attracting all traffic destined for abase station from nodes several (or more) hops away from thecompromised node. To calculate the probability of success of the SRP method, let us assume that packet size is b bytes and the preamble of thepacket is b/10 bytes in size [4]. We say packets overlap whenevera small fraction of the packet overlaps. P1 is the probabilitywith which the adversary succeeds in guessing the time atwhich the original node may send the packet.In order to make it difficult for an adversary to guess thetransmission time of a node, we can easily assume that nodestransmit packets at a random time during their allotted timeslot. Collisions can be detected when packet with strongersignal is received last.SRP Method Definition is shown in figure3. This increases the collision detectionrate to a theoretical maximum of nearly 100%. But when twopackets arrive at exactly the same time, collision cannot bedetected at all.

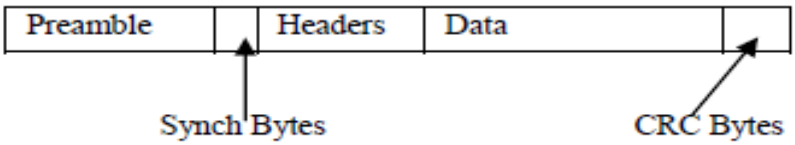

Figure3.SRP MethodDefinition

There are two possibilities in this case. (i) Both packets are lostor (ii) One with stronger signal is received.Adversary can transmit only in the time slot allocated tothe node it is trying to masquerade as. If it transmits in the timeslot that is not allocated to the node it is masquerading as, thenit is an anomaly. Thiscan be done after detecting any type of attack (not justmasquerade attacks) the primary goal of agent is to deliver information of onenode to others in the network. In order to achieve this goalwith the least overload, we put forward a least visited neighborfirst algorithm to control the navigation of mobile agent.Each node has an information cache that agents can updatewith more recent values. Nodes access this shared cachewhenever they require information about the network.

IV. WSNS CHARACTERISTICS AND WEAKNESS

Sensor networks provide unique opportunities of interaction between computersystems and their environment [6].The sensor nodes measure environmental characteristics which arethen processed in order to detect events.Most important characteristics of WSNs are including:

- Constant or mobile sensors (mobility),
- Sensor limited resources (radio communication, energy and processing),
- Low reliability, wireless communication and immunity,
- Dynamic/unpredictable WSN's topology and self-organization,
- Ad-hoc based networks,
- Hop-by-hop communication (multi-hop routing),
- Non-central management, autonomously and infrastructure-less,
- Open/hostile-environment nature and high density;

V. SECURITY ISSUES

Such attacks are relatively well-understood in software security [5]; possible countermeasures include a heterogeneous network design and standard methods from software engineering as these attacksare not characteristic for WSNs.

- Secrecy,
- Authentication,
- Privacy,
- Robustness to DoS attacks,
- Secure routing, node capture

VI. FRACTAL PROPAGATION WITH DIFFERENT FORKING PROBABILITIES

One problem with simple fractal propagation is that it generates a large amount of traffic near the base station.To address the shortcomings of MPR and RW, in thistechnique, several fake packets are created and propagatedin the network to introducemore randomness in the communication pattern. When a node hears that its neighbor nodeis forwarding a packet to the base station, the node generatesa fake packet with probability pc, and forwards it to one ofits neighbor nodes. To control the propagation range of thefake packet, each newly generated fake packet contains aTTL parameter with value K. K is a constant that is knownto all nodes. This will potentially increase the packet collision rate and packet loss rate.To addresses this problem, nodes can use different probabilities to generate fake packets [9]. When a node forwardspackets more frequently, it sets a lower probability for creating new fake packets. This technique is calledDifferential Fractal Propagation (DFP). MPR and RW spread out data traffic and make it difficultto use a rate monitoring attack. However, RW is stillvulnerable to the time correlation attack.

VII. CONCLUSION

Despite the lack of a security threat, in recent years, efforts have been made to understand and mitigate node capture and cloning attacks.The combination can be cross-layer in which multipleattacks in different layers are launched in a collaborative way. For example, theSybil attack (in the MAC and network layer) provides identity spoofing for adversariesto do the wormhole attack (in the network layer).Efficient methods to identify cloned nodesin the network are described in Still, the lack of aCommon framework prevents any discussion aboutthe degree of an attack, the network's resilience against anattack and the stability of WSNs, all of which are requiredto guarantee secure and reliable WSNs.

REFERENCES

[1] W. R. Heinzelman, J. Kulik, and H. Balakrishnan. Adaptive protocols for information Dissemination in wireless sensor networks. In Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom '99), pages 174–185, Seattle, Washington, August 1999.

[2] M. Seddigh, J. Solano Gonzalez, and I. Stojmenovic. RNG and internal node based Broadcasting algorithms for wireless one-to-one networks. Mobile Computing and Communications Review, 5(2):37–44, 2001.

[3] I. Stojmenovic. Geocasting in Ad Hoc and Sensor Networks. Technical Report TR-2004-02, Computer Science, SITE, University of Ottawa, March 2004. See also in Theoretical and Algorithmic Aspects of Sensor, Ad Hoc Wireless and Peer-to-Peer Networks, Jie Wu (ed.), CRC Press, forthcoming.

[4] M. Ilyas and I. Mahgoub, "Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems", CRCPress, 2005.

[5] A. Boukerch, L. Xu, K. EL-Khatib, "Trust-based securityfor wireless ad hoc and sensor Networks", Computer Communications, 30, 2007, pp. 2413–2427.

AUTHORS BIBLIOGRAPHY

Er. Aman dhiman was born in 1993. He received Bachelor's Degree in Electronics and communication engineering from Arni University, in 2014 and pursuing his Master's degree from Arni University. He pursues a broad range of research interests that include optical fiber communication, microwave engineering, Computer Architecture, and Cloud Computing. He has published large number of research papers

Er. Rupinder Kaur was born in 1988. She received Bachelor's Degree in Computer Engineering from Punjabi University, Patiala in 2010 and received Master's degree in Computer Science and Engineering Department from Punjabi University Patiala in 2012. She is currently working as Assistant Professor in the Department of Computer Science and Engineering in Eternal University, Himachal Pradesh, India. She pursues a broad range of research interests that include Digital Image processing, Software Engineering, Computer Architecture, and Cloud Computing. She has published large number of research papers and guided so many students for their M. Tech thesis.

Er. Manjit Thapa was born in 1987. He received Bachelor's Degree in Computer Science Engineering from Guru Nanak Dev University, Amritsar in 2009 and received master's degree in Computer Science and Engineering Department from Punjab Technical University Jalandhar in 2012. He is currently working as Assistant Professor in the Department of Computer Science and Engineering in Eternal University, Himachal Pradesh, India. He pursues a broad range of research interests that include Software Engineering, Cloud Computing, and Digital Water Marking Computer Architecture. He has published large number of research papers in international journals and presented his work at conference level and got certificates of presentation

Er. Bhubneshwar Sharma was born in 1986. He received Bachelor's Degree in Electronics and Communication Engineering from Jammu University in 2007 and received Master's degree in Electronics and Communication Department from Punjab in 2009. He is currently working as Assistant Professor in the Department of Electronics and Communication Engineering in Eternal University, Himachal Pradesh, India. He has published research papers in International Journals and presented his work at conferences. He pursues a broad range of research interests that include Digital signal processing, neural networks, Wireless sensor networks. He has also got certificates of publication of their research work.

