www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 6 June , 2013 Page No. 2055-2056

REVIEW OF INSIDIOUS ATTACKS AND ITS PROTECTION MECHANISMS FOR WIRELESS SENSOR NETWORKS

Cosmena Mahapatra [#1]

[#1] Asst. Professor, BCIIT, G.G.S.I.P.U, New Delhi

[#1]cosmenamahapatra1@gmail.com

Abstract - Wireless Sensor Network (WSN) is widely researched field which encompasses various revolutionary applications in fields like traffic management, wildlife preservation last but not the least armed forces. The addition of wireless sensor networks in various fields has also increased the security treats that have to be covered while using it. The objectives of this paper is to explore the security related issues and threats of wireless sensor networks and to propose security mechanisms for static wireless sensor networks.

Keywords— **WSN, security, sensor, challenges, proposed mechansim**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) are composed of tiny embedded computers called as 'motes' which are equipped with sensors and low-power radios and capable of self-organizing themselves into an networks that is capable of sensing physical changes in the environment such as movement of a target, temperature, humidity, etc. Due to their economical availability, WSNs are increasingly being used in diverse fields such as healthcare, environmental protection, prisons, and schools.

II. ISSUES AND THREATS TO WSN[1]

WSN requires the placement of individual nodes onto a large geographical area. The first and the foremost attack that comes into the array is the physical attack. Here the motes or the sensors are in immediate threat of being captured by hackers and crucial information being stolen from them. This information is not just restricted to data being read by the motes but may also include the private key or the public key being used for encrypting and decrypting the data being handled by the WSN. The second attack works at the network layer of WSN. This is the layer that is responsible for routing the data and localizing the sensor with in the WSN. Adding invalid routing information or including wrong localization data, can easily help the attacker to intrude into the system. Network layer attacks have been grouped under following categories:

A. *Replay Attack:* This attack causes routing loops, increases network traffic, generates false error messages, and increases network latency.

B. *Selective forwarding:* This attack results in forwarding of selected data only often which is done to include malicious node in the network.

C. *Sinkhole Attack*: Attract nearby network traffic through hacked node.

D. Wormholes: These are compromised low latency out of bound channel in WSN which force the other nodes to replay messages.

E. Hello Attack: Hello advertisement is used by pretend nodes to make the neighbours trust them

The third category of attack targets the Data link layer, that is LLC layer and the MAC Layer.Two aatcks that cen be grouped under this category are:

A. Acknowledgement Spoofing: By using LLC protocol, false acknowledgements are created to receive information from other nodes.

B. *Sybil Attack*: Here a single node posses as multiple nodes projecting the image of a group.

The attacks on transport layer nd Application layers are done in tandem with the attacks on network and Datalink layer of WSN architecture.

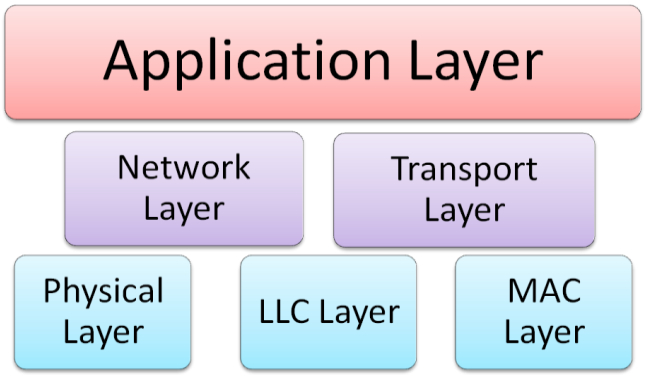

Fig 1: WSN Protocol Layers afflicted by intrusion attacks

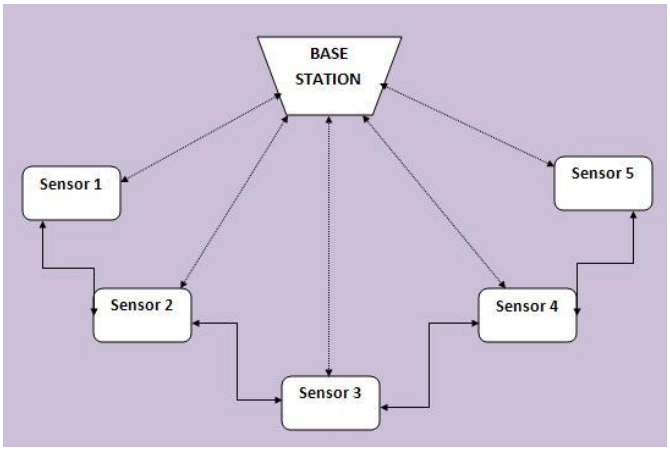

Fig 2: Hierarchical architecture for security in static WSN

III. PREVENTION OF INSIDIOUS ATTACKS IN WSN

To prevent insidious attacks from occurring in WSN, they have been grouped into two categories [3]:

A. Protect information from being detected and deciphered.
B. Providing physical protection to the motes.

In order to protect the signals from being detected at all, it has been found that if Spread spectrum technology is used in conjunction with effective power control and good directional antenna location strategy, they signals can be hidden from would be intruders. However with the growth in technology this method too has proved to be low on prevention. It has been clubbed with encryption and decryption methods so that even if the transmitted signal is detected, it can not be easily hacked into as for this the intruders would require the public key and the private key of the sender and the receiver to break into the code.

The second category of strategies pays emphasis to providing physical protection to the motes. This however is difficult to implement since the vary nature of a WSN is to spread the sensors onto a large geographical area such as a forest, where providing physical security for each node in difficult if not impossible. Some researchers have suggested the use of self destructive motes, which if tampered with would blow up their memory chip and go out of radar. This suggestion comes with a rider; sensors have a cost assigned to them. If the sensors were programmed to self destruct on slight suggestion of malice, where they might even not be one, the loss would be huge. Hence physical protection of sensors is also difficult to give.

IV. PROPOSED SECURITY ARCHITECTURE

This proposed architecture is only for static WSN where the motes/sensors would be connected to each other in a hierarchical format. This means each mote knows its successor node and predecessor node via a Secret ID (SE-ID). This SE-ID can be anything starting from the X, Y location of the sensor, weight of the sensor or any randomly generated alphanumeric ID. The SE-ID of each Mote would be exchanged only once in the starting, i.e. when the network was being established. The exchange would be done through the use of a stable key exchange encryption algorithm, making it difficult for the attacker to decrypt it. Once the SE-ID have been exchanged, then only the transmission can be triggered between the base station and the motes. If an intruder tries to install a new mote or change the configuration of the current mote, he would have to be aware of the secret id of the successor mote or the predecessor mote for him to do so.

V. CONCLUSIONS

WSN security is threatened by many safety challenges. The proposed architecture in this paper helps to manage the physical safety of the network topology by via a low cost and simple solution.

VI. FUTURE SCOPE

The proposed architecture is useful only for static WSN, where the motes are not in movement. However work is still left to make it adaptable for Adhoc WSN which are increasingly being used in our daily life.

REFERENCES

[1] *Gordon W Skelton, "Cyber-Physical Security for wireless sensor networks", CDID ,2010*
[2] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in wireless sensor networks: Issues and challenges", ICACT, 2006.
[3] Kamran Jamshaid ,"A Framework for implementing security is wireless sensor networks", Thesis,2002.
[4] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Comput. Netw. J., vol. 38, no. 4, Mar. 2002, pp. 393– 422.M.
[5] J. Polastre , R. Szewczyk , D. Culler, "Telos: enabling ultra-low power wireless research," Proceedings of the 4th international symposium on Information processing in sensor networks, Los Angeles, California, April 24-27, 2005.
[6] D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, and D. Culler, "The nesC language: a holistic approach to networked embedded systems", In Proceedings of SIGPLAN 2003 Conference on Programming Language Design and Implementation (PLDI), New York, NY, USA, pp.1–11, 2003.