Security For Wireless Sensor Network

Saurabh Singh
Department of Computer Science and Engineering, NIT Jalandhar
Punjab, India

Dr. Harsh Kumar Verma
Department of Computer Science and Engineering, NIT Jalandhar
Punjab, India

***Abstract*— Wireless sensor network is highly vulnerable to attacks because it consists of various resource-constrained devices with their low battery power, less memory, and associated low energy. Sensor nodes communicate among themselves via wireless links. However, there are still a lot of unresolved issues in wireless sensor networks of which security is one of the hottest research issues. Sensor networks are deployed in hostile environments. Environmental conditions along with resource-constraints give rise to many type of security threats or attacks. Securely communication among sensor nodes is a fundamental challenge for providing security services in WSNs. This paper gives the security of wireless sensor network and attack at different layered architecture of WSN and their prevention.**

Keywords- Sensor network, security, attack, communication protocol, defense.

I. INTRODUCTION

Wireless sensor network (WSN) defined as a network of possibly low-size, low-battery power and low-complex devices denoted as nodes that can sense the environment and communicate the information gathered from the monitored field through wireless links [2, 3], the sensed data is forwarded, possibly via multiple hops relaying, to a sink that can use it locally, or is connected to other networks through a gateway. It is a rapidly emerging field which will have a strong impact on research and will become an integral part of our lives in the near future. The huge application space of WSNs covers national security, surveillance, military, health care, environment monitoring and many more. Due to their wide-range of potential applications, WSNs have attracted considerable research interest in recent years.

Such networks have substantial data acquisition and data processing capabilities and for this reason is deployed densely throughout the area where they will monitor specific phenomena. However, due to the lack of tamper-resistant packaging and the insecure nature of wireless communication channels, these networks are vulnerable to internal and external attacks [15, 12, 9]. Adversary can physically capture and get the information contained in the sensor node, eavesdrop and inject new messages, modify messages. Hence there must be some sort of mechanism for node to node securely data transmission.

II. SENSOR NETWORK COMMUNICATION ARCHITECHURE

The sensor nodes are usually scattered in a sensor field. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink and the end users. Data are routed back to the end user by a multi hops infrastructure less architecture through the sink. The sink may communicate with the task manager node via Internet or Satellite.

The task manager or base station is centralized point of control within the network, which extracts information from the network and disseminates control information back into the network. It also serves as a gateway to other networks, a powerful data processing/storage centre and an access point for a human interface. Hardware- wise the base station is either a laptop or a workstation.

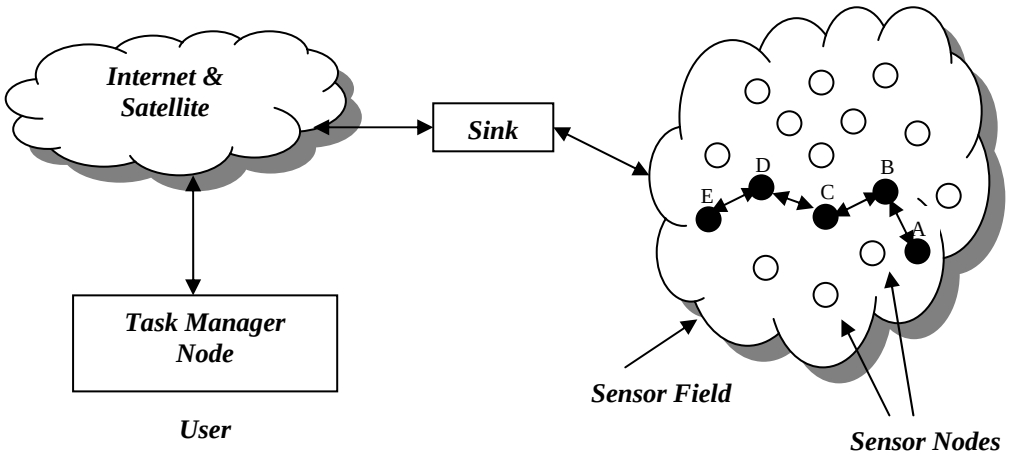

Fig 1: Sensor Network Communication Structure [12,13]

III. APPLICATION OF WSN

Wireless sensor network are being deployed widely and they gives an economical solution to many problem. In this section gives a nice survey on applications of Wireless Sensor Networks. Here some typical and promising applications of WSNs [2,7].

A. Military applications:

It can be used For commanders to monitor the status (position, quantity, availability) of their troops, equipment and battlefield surveillance or reconnaissance of opposing forces and terrain to target the enemy, to detect biological and chemical attack.

B. Environmental applications:

It can be used To monitor the condition/status of environment such as humidity, temperature, pressure, and pollution in soil, marine, and atmosphere. Also detect a disaster such as forest fire, flood, tsunami, volcano activities that is about to happen.

C. Health applications:

It can be used to remotely monitor/track/diagnose the condition/status (position, quantity, heart rate, blood pressure) of doctor, patient or drug, equipment, etc.

D. Commercial applications:

It can be used to detect/track/monitor vehicles, to manage/control inventory/warehouse, to support interactive devices, or to control environment of a building.

E. Scientific exploration:

WSNs can be deployed under the water or on the surface of a planet for scientific research purpose.

F. Area monitoring:

In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. For example, a large quantity of sensor nodes could be deployed over a battlefield to detect enemy intrusion instead of using landmines. When the sensors detect the event being monitored (heat, pressure, sound, light, electro-magnetic field, vibration, etc), the event needs to be reported to one of the base stations, which can take appropriate action (e.g., send a message on the internet or to a satellite).

IV. SECURITY REQUIREMENT

Since sensor networks are used for many applications where security is crucial. It is essential to ensure secure communication among the nodes. It is not possible to use general secure communication techniques for WSNs because of resource-constraints and communication overheads involved[13]. The security requirement of wireless sensor network can be classified as follows:

A. Authenticity:

Authentication is important application in sensor networks. Adversary can easily inject messages, the receiver needs to ensure that data used in any decision making process originate from trusted source. Authentication allows sender node and receiver must be sure that they talking really to the node to which they want to communicate.

B. Confidentiality:

Confidentiality guarantee that data sent on the channel will not be read correctly by anybody other than communicating nodes. For this purpose, the message is sent on the channel in encrypted form. Confidentiality means keeping information secrete from unauthorized parties.

C. Integrity:

Integrity means that the data should not be modified by adversary to the receiver. If it happens, then receiver must verify that data received is exactly the same as sent by the sender. For that purpose, a message authentication code (MAC) is generated by the sender using some MAC key and that is sent with the encrypted message. At the other end, the receiver will verify the authenticity of the received message by using that MAC key.

D. Scalability:

The key management scheme, should be scalable in the sense that if network size grows, it should not increase the chances of node compromise, should not increase communication overhead. It should allow nodes to be added in network after the deployment as well.

V. SENSOR NETWORK PROTOCOL

Wireless sensor network protocol used by the sink and all sensor nodes. This protocol stack combines power and routing awareness, integrates data with networking protocols, communicates power efficiently through the wireless medium, and promotes cooperative efforts of sensor nodes. The protocol stack consists of the application layer, transport layer, network layer, data link layer, physical layer, power management plane, mobility management plane, and task management plane.

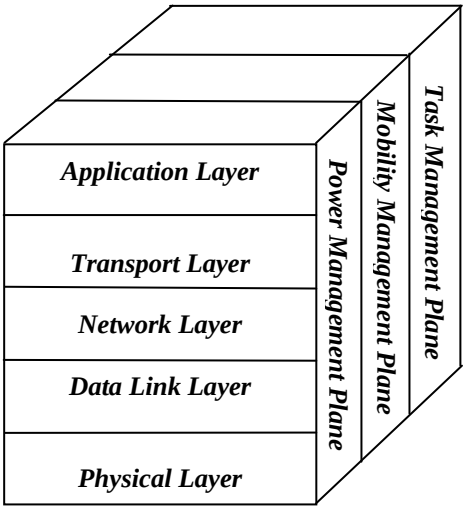

Fig 2: Sensor networks protocol stack[6,10]

A. Physical Layer:

The physical layer addresses the needs of a simple but robust modulation, transmission and receiving techniques such as Ultra Wideband, Impulse Radio and Pulse Position modulation have been used to reduce complexity and energy requirements, whilst improving reliability and reducing path loss and shadowing[8]. In addition, it established connection, data rate, data encryption, frequency generation and signal detection.

B. Data Link Layer:

The Data Link Layer is responsible for medium access, error control, multiplexing of data streams and data frame detection. It ensures reliable point to point and point to multi hop connections in the network. DLL detect and correct the transmission errors using error correction method. This layer is vulnerable to data collision when more than one sender tries to send data on a single transmission channel.
Data link layer protocols include, SMACS (Self-Organized Medium Access Control for Sensor Networks), EARS (Eavesdrop and Register)[11].

C. Network Layer:

The Network Layer is responsible for intra-network operation, different type addressing routing information through the sensor network, finding the most efficient path for the packet to travel on its way to a destination. It handles the routing of the data and forwarding from node to base station and vice versa[11,17].
To save the power of sensor so as to increase the life of sensor, network layer use SMECN (Small Minimum Energy Communication Network) and LEACH (Low Energy Adaptive Clus- tering Hierarchy) protocol .

D. Transport Layer:

This layer is responsible for reliable end –to-end data transfer. The transport layer performs the service of sending and receiving of data to sensor network connected to the internet. This is the most challenging issue in wireless sensor network.

E. Application Layer:

The Applications Layer is responsible presenting all required information to the application and propagating requests from the application layer down to the lower layers. It contain service element to support application process such as data collection, management and the processing of the data through the application software for getting reliable result.
Some preliminary protocols in this area include SMP (Sensor Management Protocol), TADAP (Task Assignment and Data Advertisement Protocol), and SQDDP (Sensor Query and Data Dissemination Protocol).

VI. Attack On Wsn Layer And Their Defence

A. Physical Layer Attacks:

Jamming and tampering are the most common attacks to the physical layer of a WSN.

- *Jamming Attacks:*

Interferes with the radio frequencies the nodes are using. Only a few jamming nodes can put a considerable amount of the nodes out of order. If the adversary can block the entire network then that constitutes complete DoS. However, larger networks are harder to block in their entirety.

In such jamming attacks however it would be ideal if the nodes under attack could alert the rest of the network and ideally the base station about what is going on. Jammed nodes should attempt to inform neibouring nodes of the attack during jamming gaps and these nodes should in turn inform the base station. Neighbouring nodes can also assume a jamming attack if they observe change in the neighbouring background noise.

- *Tampering Attack:*

Attacker may damage a sensor, replace the entire node or part of its hardware or even electronically interrogate the nodes to gain access to sensitive information, such as shared cryptographic keys and how to access higher communication layers.

The ideal solution to tampering is providing tamper resistant packaging for the motes. This however is a very costly procedure which needs to be considered during design time and will no doubt increase the average price of motes. Camou aging is another option. The motes may also be programmed to erase sensitive data upon capture.

B. Data Link Layer Attacks:

Collisions, unfairness or exhaustion attacks can be launched against the data link layer of a sensor network.

- *Collisions Attack*

A type of link layer jamming. If an attacker can corrupt an octet of transmission such that a checksum mismatch occurs, then the entire packet can be disrupted[17].

Collision detection is the obvious solution here, however it hasn't yet been less effective[20]. One may choose to employ error correcting codes, however these can be easily corrupted and require extra overhead bits.

- *Exhaustion Attack*

This occur when naive link layer implementations attempt repeated retransmission even after unusually late collisions. A variation of this attack is when a self sacrificing node continuously ask for access to a channel, forcing its neighbours to respond with a clear to send message.

Time division multiplexing can solve the problem of indefinite postponement during collisions. MAC admission control rate limiting is a measure by which the link layer can ignore excessive requests without having to send radio messages.

C. Network Layer Attacks:

- *Selective Forwarding:*

In such an attack the adversary includes himself/herself in a data own path of interest. Then the attacker may choose not to forward certain packets and drop them causing a sort of black hole. A variation of this attack is when the adversary only drops packets coming from a specific source whilst reliably forwarding other packets. Such attacks are much harder to detect than black hole attacks[9,11].

The solution to selective forwarding attacks is to introduce redundancy to the network in the form of multi-path routing. In such circumstances a message is routed over n paths, and hopefully one message will travel along a path that is disjoint from the selective forwarding node.

- *Sinkhole Attacks:*

The goal of a sinkhole attack is to lure tra c to a malicious part of the network. Such attacks are usually the launching block for other attacks such as selective forwarding. Sinkholes work by making a compromised node attractive to its neighbours. This is done by advertising high quality routes i.e low latency routes. Fooled neighbours will then forward all their data destined to the base station to the lying node. Sensor networks are susceptible to these attacks due to their multihop nature and the specialised communication patterns they use.

- *The Sybil Attack:*

The Sybil attack targets[4,6] fault tolerant schemes such as distributed storage, dispersity, multipath routing and topology maintenance. This is done by having a malicious node present multiple identities to the network. This attack is especially confusing to geographic routing protocols as the adversary appears to be in multiple locations at once.

An insider cannot be prevented from participating in a network. However, he should only be allowed to do so using identities he has compromised and no more. The solution here is to verify the identities of participating nodes. This can be done by having each node share a unique key with the base station. Two

neighbouring nodes then communicate with each other using a shared key to encrypt and verify the link between them. Note that this technique does not stop a compromised node from communicating with the base station or other aggregations points but it definitely limits the number of legitimate nodes the compromised node can communicate with. The base station can help enforce this principle by limiting the number of verified neighbours a node can have and generating an error when this number is exceeded.

- *Wormholes:*

In these attacks the adversary tunnels messages received in one part of the network over a low latency link, to another part of the network where the messages are then replayed. The simplest occurrence of this attack is to have a malicious node forwarding data between two legitimate nodes. Wormholes often convince distant nodes that they are neighbours, leading to quick exhaustion of their energy resources[7,4,6]. An attacker close to the base station can completely disrupt routing by creating well positioned wormholes that convince nodes multiple hops from the base station that they are only a couple of hops away through the wormhole. When this attack is coupled with selective forwarding and the Sybil attack it is very difficult to detect.

These are the hardest attacks to defend against because wormholes use channels that are invisible to the network and the advertised routes of sinkholes are extremely hard to verify. Geographic routing protocols however are resistant to these attacks because messages are routed towards the physical location of the base station. False links will be detected by neighbours that figure out that the physical distance of an advertised route exceeds the radio signal range of motes. Another solution would be to provide tight time synchronization which is often not feasible and requires original protocol design by which to make these attacks useless.

- *Hello Flood attacks:*

In many routing protocols, nodes broadcast hello messages to announce their presence to their neighbours[18]. A node receiving such a message can assume that the node that sent the message is within it's range. An attacker with a high powered antenna can convince every node in the network that it is their neighbour. If the attacker also advertises a high quality route it can get every node to forward data to it. Nodes at a large distance from the attacker will be sending their messages into oblivion leaving the network in a state of confusion. This attack can also be thought of as a type of broadcast wormhole. Routing protocols dependant on localised information are extremely vulnerable to such attacks.

Such attacks can easily be avoided by verify bi-directionality of a link before taking action based on the information received over that link. The Needham-Schroeder verification protocol [15] does just that. If the base station limits the number of verified neighbours it can prevent this attack all together.

- *Acknowledgement Spoofing:*

Protocols that choose the next hop based on reliability issues are suspect able to acknowledgments spoofing [7,8]. Here the attacker spoofs acknowledgement convincing the sender that a weak link may be strong or a dead node is alive. This results in packets being lost when traveling along such links.

The most obvious solution to this problem would be authentication via encryption of all sent packets and also packet headers [12]. The idea is that no node should be able to spoof messages from the base station, yet every node should be able to verify the identity of the base station.

VII. CONCLUSION

In this paper we presented wireless sensor network, security requirement and different type of attack and their prevention mechanism at different layered protocol stack of wireless sensor network. This paper gives brief introduction of WSN, sensor network communication architecture and some application of wireless sensor network.

VIII. ACKNOWLEDGMENT

The author would like to thanks the anonymous referess for their valuable comments, which greatly improved the readability of the paper.

REFERENCES

[1] A. D. Wood and J. A. Stankovic(2002) "Denial of service in sensor networks", Computer, 35(10):54–62, 2002.

[2] A. Perrig, R. Szewczyk, V. Wen et al.,"SPIN:security protocols for sensor network," Wireless Network,Vol.8.,No.5,pp. 521-534,2002.

[3] A. K. Pathan, H. W. Lee, and C. S. Hong, " Security in wireless sensor network: issues and challenges," In proceeding of the 8th ICACT 06,Volume 2, Phoenix Park, Korea, pp. 1043-1048,February, 2006

[4] Chris Karlof, Naveen Sastry, David Wagner, (2004)Tiny Seca link layer security architecture for wireless sensor networks, Proceedings of the 2nd international conference on Embedded networked sensor systems

[5] Al-Sakib khan Pathan et.al,(2006) "Security in wireless sensor networks: Issues and challenges" in feb.20-22,2006,ICACT2006,ISBN 89-5519-129-4 pp(1043-1048)

[6] Abhishek Panday, R. C. Tripathi, "A Survey on Wireless Sensor Network Security" International Journal oComputer Application(0975-8887) Volume 3- No.2, June 2010

[7] Adrian Perrig, John Stankovic, and David Wagner, (2004) "Security in wireless sensor networks" Commun.ACM,47(6):53-57.

[8] Jinat Rehana, "Security of Wireless Sensor Network" TKK T-110.5190 Seminar on Internetworking, April 2009

[9] A. D. Wood and J. A. Stankovic,(2002) "Denial of service in sensor networks",Computer, 35(10):54–62, 2002.

[10] Kalpana Sharma, M K Ghose "Wireless Sensor Network: An Overview on its Security" IJCA Special Issue on "Mobile Ad-hoc-Network" MANETs 2010

[11] Mayank Saraogi . Security in Wireless Sensor Networks. In ACM SenSys, 2004.

[12] S. Datema. A Case Study of Wireless Sensor Network Attacks. Master's thesis, Delft University of Technology, September 2005.

[13] Sophia Kaplantzis, "Security Models for Wireless Sensor Networks" March 20, 2006

[14] C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems, pages 162–175, New York, NY, USA, 2004. ACM Press.

[15] Adrian Perrig, Robert Szewczyk, J.D. Tygar, Victor Wen, "SPINS: Security Protocols for Sensor Networks", Department of Electrical Engineering and Computer Sciences, University of California, Berkley, 2002.

[16] Kirk H.M. Wong, Yuan Zheng, Jiannong Cao, Shengwei Wang," A Dynamic User Authentication Scheme for Wireless Sensor Networks", IEE International Conference on Sensor Networks Ubiquitous and Trustworthy Computing (SUTC"06), 2006.

[17] Chris Karlof David Wagner. In Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

[18] Z. Tanveer and Z. Albert. Security issues in wireless sensor networks. In ICSNC '06: Proceedings of the International Conference on Systems and Networks Communication, page 40, Washington, DC, USA, 2006. IEEE Computer Society.

[19] D. R. Raymond and S. F. Midkiff. Denial-of-service in wireless sensor networks: Attacks and defenses. In IEEE Pervasive Computing, volume 7, pages 74–81, 2008.

[20] Chee-Yee Chong and Srikanta P. Kumar, "Sensor Networks: Evolution, Opportunities and Challenges". Proceeding of the IEEE, vol. 91, no. 8, Aug. 2003.

[21] W. Heinzelman, A. Chandrakasan and H. Balakrishnan. "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Transactions on Wireless Communications,Vol. 1, No. 4, 660-670, October 2002.

AUTHORS PROFILE

Saurabh Kumar Singh He received B.Tech degree in computer science and engineering in 2009 from Institute of Engineering and Technology Jhansi, India. Currently he is pursuing M.Tech degree,in computer science and engineering from National Institute of Technology Jalandhar India in 2009 and 2011 respectively.

He is Microsoft Certified Professional, His current research include in wireless sensor network, computer network and information security.

Dr. Harsh K Verma He has completed Phd in Numerical Computing from Punjab Technical University Punjab, India. He is currently a professor and Head of Department of computer science and engineering in National Institute of Technology Jalandhar India.

His research include in numerical computing, information security and computer networks. he has published various paper in national and international journal and conferences. He has attended various national and international workshop training schools and other technical activity during his academic carrier.