International Journal For Technological Research In Engineering *ISSN (Online): 2347 - 4718*
International Conference on Emerging Technologies in Engineering, Biomedical, Medical and Science (ETEBMS - 16)

WIRELESS SENSOR NETWORKS: SECURITY ISSUES

Musbahu Muhammad Adam[1], Nura Muhammad Shehu[2]
Master's Scholars, Department of Electronics and Comm. Engineering JNU, Jodhpur

Abstract: Wireless Sensor Network (WSN) is an emerging technology that shows great promise for various futuristic applications both for mass public and military. The sensing technology combined with processing power and wireless communication makes it lucrative for being exploited in abundance in future. Wireless sensor networks consist of small nodes with sensing, computation, and wireless communications capabilities. As wireless sensor networks continue to grow, so does the need for effective security mechanisms. Because sensor networks may interact with sensitive data and operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design. However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network security. We consider routing security in wireless sensor networks. Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. We propose security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks — sinkholes and HELLO floods, and analyze the security of all the major sensor network routing protocols. The intent of this paper is to investigate the security related issues and challenges in wireless sensor networks. We identify the security threats, review proposed security mechanisms for wireless sensor networks.
Keywords: WSN, TinyOS beaconing, GEAR.

I. INTRODUCTION

Our focus is on routing security in wireless sensor networks. Current proposals for routing protocols in sensor networks optimize for the limited capabilities of the nodes and the application specific nature of the networks, but do not consider security. Although these protocols have not been designed with security as a goal, we feel it is important to analyze their security properties. When the defender has the liabilities of insecure wireless communication, limited node capabilities, and possible insider threats, and the adversaries can use powerful laptops with high energy and long range communication to attack the network, designing a secure routing protocol is non-trivial. We present crippling attacks against all the major routing protocols for sensor networks. Because these protocols have not been designed with security as a goal, it is unsurprising they are all insecure. However, this is non-trivial to fix: it is unlikely a sensor network routing protocol can be made secure by incorporating security mechanisms after design has completed. Our assertion is that sensor network routing protocols must be designed with security in mind, and this is the only effective solution for secure routing in sensor networks.

A. Wireless Sensor Network:

A wireless sensor network is a collection of nodes organized into a network. Each node consists of processing capability, may contain multiple types of memory, have a RF transceiver (usually with a single omni- directional antenna), have a power source, and accommodate various sensors and actuators. The nodes communicate wirelessly and often self-organize after being deployed in an ad hoc fashion. Systems of 1000s or even 10,000 nodes are anticipated. Many routing, power management, and data dissemination protocols have been specifically designed for WSNs where energy awareness is an essential design issue.

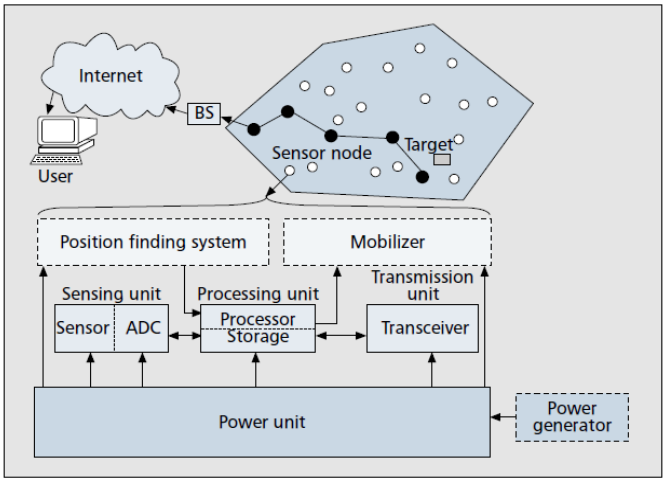

Fig. 1.1 The components of a sensor node

B. Protocols:

Sensor nodes like any other telecommunications device adhere to a specific protocol stack (Fig.1.2). Layered network architectures are adopted because they most certainly always improve the robustness of a system. In this section, we specify the task of each layer of the stack and the most common protocols coupled with each layer [3].

Note that a lot of research is still being conducted in perfecting the protocol stack for sensor network, so the exact protocols are yet to be concreted.

The *Physical Layer* is responsible for carrier frequency generation, frequency selection, signal detection, modulation and data encryption. 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 effects and shadowing.

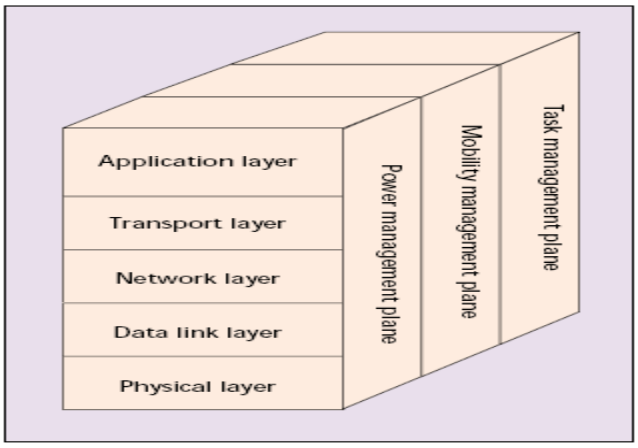

Fig. 1.2 : Sensor Node Protocol Stack

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 multihop connections in the network. Due to the network constraints conventional MAC protocols are not suited to sensor networks. Some widespread data link layer protocols include: SMACS (Self-Organised Medium Access Control for Sensor Networks) [7], EARS (Eavesdrop and Register) , CSMA-Based medium Access Protocols [8] and Hybrid TDMA/FDMA-Based protocols [9].

The Network Layer is responsible for routing information through the sensor network i.e. finding the most efficient path for the packet to travel on its way to a destination. Most protocols can be categorised under one of the following techniques: gossiping, flooding, SMECN (Small Minimum Energy Communication Network) [10], SPIN (Sensor Protocols for Information via Negotiation) [11], SAR (Sequential Assignment Routing) [7], LEACH (Low Energy Adaptive Clustering Hierarchy) [12] and Directed Diffusion [13].

The Transport Layer is needed when the sensor network intends to be accessed through the internet. However, no scheme has been devised to fully address this issue. Modified TCP/UDP like protocols may be an appropriate solution but this is yet to be established.

The Applications Layer is responsible presenting all required information to the application and propagating requests from the application layer down to the lower layers. Some preliminary protocols in this area include SMP [14](Sensor Management Protocol), TADAP (Task Assignment and Data Advertisement Protocol) [14], and SQDDP (Sensor Query and Data Dissemination Protocol) [14].

II. ATTACKS ON SENSOR NETWORK

Many sensor network deployments are security sensitive and attacks against them provoke the possibility for real-world damage to the health and safety of people. Hardware failures, bugs, resource exhaustion, malicious attacks and environmental conditions can diminish or even eliminate a networks capacity to perform as expected. Such conditions are defined as Denial of Service (DoS) attacks in the literature. In the previous section we outlined the layered network architecture of sensor networks. In this section we specify DoS vulnerabilities to the first four layers of the stack (Figure4), as specified in studies conducted by Wood and Stankovic [2].

A. Physical Layer Attacks: Jamming and tampering are the most common attacks to the physical layer of a WSN.

- Jamming 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.
- Nodes may fall victims to physical tampering, especially if they are part of a network that covers a vast area. A tampering 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.

B. Data Link Layer Attacks: Collisions, unfairness or exhaustion attacks can be launched against the data link layer of a sensor network.

- Collisions are 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. Corrupted ACK messages usually lead to costly exponential backoff in some MAC protocols. A compromised node may also intentionally deny access to a channel, whilst expending less energy required by full-time jamming of the channel.
- Unfairness is a weaker form DoS that is done by abusing MAC priority schemes. Such an attack usually leads to loss of real-time deadlines and hence degradation of service.
- Exhaustion of battery resources may 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.

C. Network Layer Attacks: Wood and Stankovic [2] inform us that neglect, greed, homing, misdirection, authorisation, probing, blackholes and monitoring are possible routing layer attacks. In a later more detailed study, Karlof and Wagner [20] put specific names and methodologies to these attacks.

- Spoofed, altered or replayed routing information: This is the most direct attack. By spoofing, altering or replaying routing information the attacker can complicate the network by creating routing loops, attracting or repelling traffic, generating false error

messages, shortening or extending source routes or partitioning the network.

- Selective Forwarding: In such an attack the adversary includes himself/herself in a data flow 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.
- Sinkhole Attacks: The goal of a sinkhole attack is to lure traffic 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 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.
- 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. 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.
- Hello flood attacks: In many routing protocols, nodes broadcast hello messages to announce their presence to their neighbours. 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.
- Acknowledgement Spoofing: Protocols that choose the next hop based on reliability issues are suspectable to acknowledgments spoofing. 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.

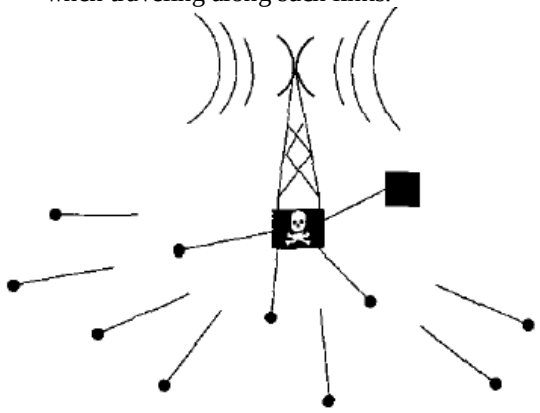

Fig. 2.1. Hello Flood Attack

D. Transport Layer Attacks: Finally the transport layer can be attacked via flooding or desynchronisation.

- The goal of flooding attacks is to exhaust memory resources of a victim system. Similar to TCP SYN attacks the attacker sends many connection establishment requests, forcing the victim to allocate memory in order to maintain the state for each connection.
- In desychronisation attacks the hacker forges messages between endpoints. Control flags and sequence numbers are usually modified. If the attacker can get the timing right, he might prevent the endpoints from ever exchanging messages as they will be continually requesting retransmission of previous erroneous messages.

This attack leads to an infinite cycle that wastes energy.

A. Attacks on specific protocols

a) Tiny OS beaconing : It constructs a 'Breadth first' spanning tree rooted at the base station. Base station periodically broadcast route updates from immediate nodes to parent, base station; other nodes to parent, from who they receive the first update. Packets travel through the paths along tree.

Attacks:

Unauthenticated route updates : In this malicious node acts as base station.

Authenticated route updates : In this two colluding nodes (laptop-class attacker) form wormhole to direct all traffic

through them. Laptop-class attacker use HELLO flood attack in which every node marks attacker as parent. Mote-class attacker can cause 'Routing loops' between two nodes.

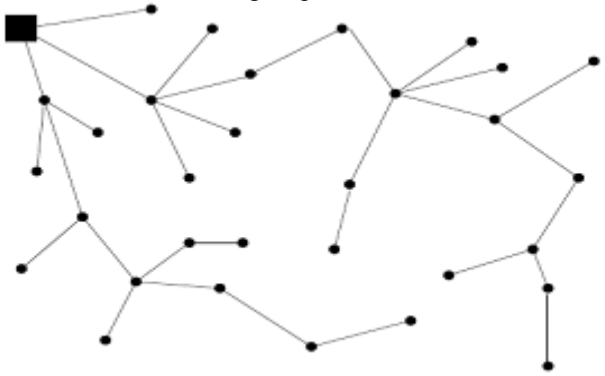

Fig. 2.2 A representative topology constructed using TinyOS beaconing with a single base station.

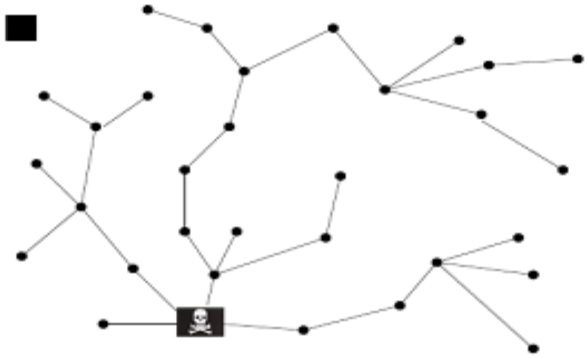

Fig. 2.3 An adversary spoofing a routing update from a base station in TinyOS beaconing.

Fig. 2.4 A laptop-class adversary using a wormhole to create a sinkhole in TinyOS beaconing.

b) Directed diffusion: In directed diffusion, sensors measure events and create gradients of information in their respective neighborhoods. The BS requests data by broadcasting interests. An interest describes a task required to be done by the network. An interest diffuses through the network hop by hop, and is broadcast by each node to its neighbors. As the interest is propagated throughout the network, gradients are set up to draw data satisfying the query toward the requesting node (i.e., a BS may query for data by disseminating interests and intermediate nodes propagate these interests). Each sensor that receives the interest sets up a gradient toward the sensor nodes from which it receives the interest. This process continues until gradients are set up from the sources back to the BS.[15]

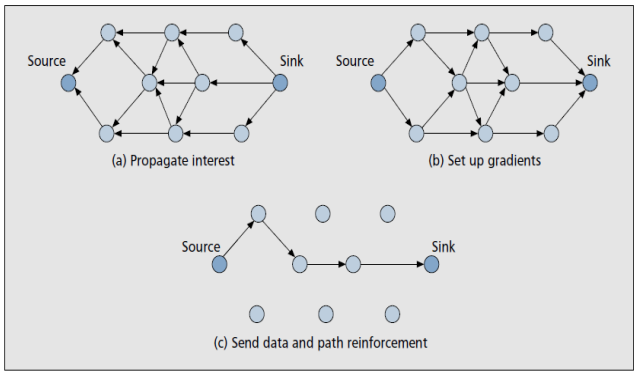

Fig. 2.5 An example of interest diffusion in a sensor network.

Figure 2.5 shows an example of the working of directed diffusion (sending interests, building gradients, and data dissemination). When interests fit gradients, paths of information flow are formed from multiple paths, and then the best paths are reinforced to prevent further flooding according to a local rule. In order to reduce communication costs, data is aggregated on the way. The goal is to find a good aggregation tree that gets the data from source nodes to the BS.

Attacks : Cloning i.e. Replay of interest by the adversary. Selective forwarding and data tampering

c) Geographic Adaptive Fidelity : GAF is an energy-aware location-based routing algorithm designed primarily for mobile ad hoc networks, but may be applicable to sensor networks as well. The network area is first divided into fixed zones and forms a virtual grid. Inside each zone, nodes collaborate with each other to play different roles. For example, nodes will elect one sensor node to stay awake for a certain period of time, and then the rest go to sleep. This node is responsible for monitoring and reporting data to the BS on behalf of the nodes in the zone. Each node uses its GPS-indicated location to associate itself with a point in the virtual grid. Nodes associated with the same point on the grid are considered equivalent in terms of the cost of packet routing. Such equivalence is exploited in keeping some nodes located in a particular grid area in sleeping state in order to save energy. Thus, GAF can substantially increase the network lifetime as the number of nodes increases. There are three states defined in GAF:

i) discovery, for determining the neighbors in the grid;
ii) active, reflecting participation in routing; and
iii) sleep, when the radio is turned off.[17]

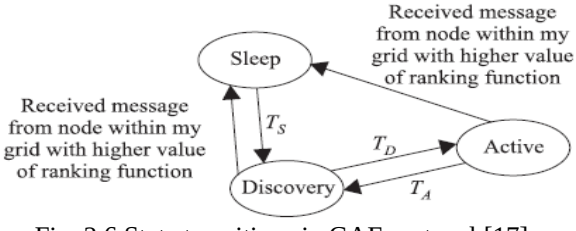

Fig. 2.6 State transitions in GAF protocol.[17]

d) Geographic and Energy Aware Routing : This provides the use of geographic information while disseminating queries to appropriate regions since data queries often include geographic attributes. The protocol, Geographic and Energy Aware Routing (GEAR), uses energy-aware and geographically informed neighbor selection heuristics to route a packet toward the destination region. The key idea is to restrict the number of interests in directed diffusion by only considering a certain region rather than sending the interests to the whole network. By doing this, GEAR can conserve more energy than directed diffusion. Each node in GEAR keeps an estimated cost and a learning cost of reaching the destination through its neighbors. The estimated cost is a combination of residual energy and distance to destination. The learned cost is a refinement of the estimated cost that accounts for routing around holes in the network. A hole occurs when a node does not have any closer neighbor to the target region than itself. If there are no holes, the estimated cost is equal to the learned cost. The learned cost is propagated one hop back every time a packet reaches the destination so that route setup for the next packet will be adjusted. There are two phases in the algorithm:

- Forwarding packets toward the target region: Upon receiving a packet, a node checks its neighbors to see if there is one neighbor that is closer to the target region than itself.
- Forwarding the packets within the region: If the packet has reached the region, it can be diffused in that region by either recursive geographic forwarding or restricted flooding.

Attack: Location information misrepresented that means Adversary advertise wrong location information so as to place himself in the path. Adversary forge location advertisements creating routing loops. In GEAR, energy is also considered so adversary advertise maximum energy (Laptop class attacker again)

III. CONCLUSION

Routing in sensor networks is a new area of research, with a limited but rapidly growing set of research results. The common objective of trying to extend the lifetime and security of the sensor network while not compromising data delivery. Secure routing is vital to the acceptance and use of sensor networks for many applications, but we have demonstrated that currently proposed routing protocols for these networks are insecure. We leave it as an open problem to design a sensor network routing protocol that satisfies our proposed security goals. Link layer encryption and authentication mechanisms may be a reasonable first approximation for defences against mote-class outsiders, but cryptography is not enough to defend against laptop-class adversaries and insiders: careful protocol design is needed as well.

REFERENCES

[1] T. Rappaport, "Wireless Communications: Principles and Practice," Prentice Hall, 2002.
[2] Jamal N. Al-Karaki and Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", Wireless Communications IEEE, Vol. 11, Issue 6, pp. 6-28, December 2004.
[3] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communication Magazine, Aug. 2002.
[4] K. Akkaya and M. Younis, "A survey of routing protocols in wireless sensor networks", Elsevier Ad Hoc Network Journal, vol. 3, no. 3, pp. 325--349, 2005.
[5] C. Schurgers and M.B. Srivastava, "Energy Efficient Routing in Wireless Sensor Networks," MILCOM Proc. Commun. for Network-Centric Ops.: Creating the Info.Force, McLean, VA, 2001.
[6] J. Schiller, Mobile Communications. Addison Wesley Publishers, 2006.
[7] E. e. a. Sohrabi, "Protocols for self-organization of a wireless sesnor network," pp. 16–27, October 2000.
[8] Woo and D. Culler, "A transmission control scheme for media access in sensor networks.," July.
[9] E. Shih and et al, "Physical layer driven protocol and algorithm design for energy efficient wireless sensor networks," July.
[10] L. Li and J. Halpern, "Minimum- energy module wireless networks revisited," June 2001.
[11] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," pp. 174–185, 1999.
[12] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy efficient communication protocol for wireless microsensor networks," in The 33rd Annual Hawaii International Conference on System Siences (HICSS-33), Jan 4-Jan 7 2000, Proceedings of the Hawaii International Conference on System Sciences, (Maui, USA), p. 223, IEEE, Los Alamitos, CA, USA, 2000.
[13] C. Intanagowiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," pp. 56–67, 2000.
[14] C. Shen, C. Srisatjapornphat, and C. Jaikaeo, "Sensor information networking architecture and applications," IEEE Pers. Communication, pp. 52–59, Aug. 2001.
[15] C. S. Raghavendra, K. M. Sivalingam, and T. Znati, Wireless Sensor Networks. Springer Academic Publishers, 2004.
[16] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed Diffusion: a Scalable and Robust Communication Paradigm for Sensor Networks Proc. ACM Mobi- Com 2000, Boston, MA, 2000, pp. 56–67.

[17] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," Proc. 5th ACM/IEEE Mobicom, Seattle, WA, Aug. 1999. pp. 174–85.
[18] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation- Protocols for Disseminating Information in Wireless Sensor Networks Wireless Networks, vol. 8, 2002, pp. 169–85. 2009.

