International Journal of Scientific & Engineering Research, Volume 8, Issue 4, April-2017
ISSN 2229-5518

Wireless Sensor Networks

V.Swathy, J.Nisha Mary Gracea, S.Shobana.

ABSTRACT: Computer network is a group of computing devices like computers which are connected together and these devices communicate or exchange the information through links. One such type of network is wireless sensor networks. Wireless sensor networks.

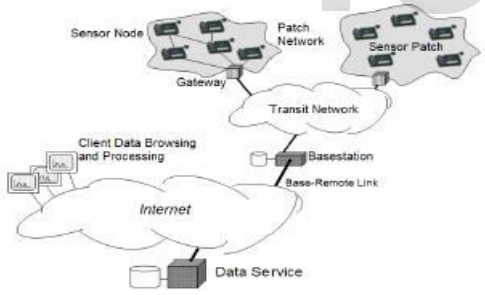
OBJECTIVE: "A wireless sensor network (WSN) is a network made of numerous small independent sensor nodes. The sensor nodes, typically the size of a 35 mm, are self-contained units consisting of a battery, radio, sensors, and a minimal amount of on-board computing power. The nodes self-organize their networks, rather than having a pre-programmed network topology. Because of the limited electrical power available, nodes are built with power conservation in mind, and generally spend large amounts."

INTRODUCTION:

We use the term sensor network to refer to a heterogeneous system combining tiny sensors and actuators with general purpose computing elements. The Application domains of Wireless Sensor Network are diverse due to the availability of micro-sensors and low-power wireless communications. Unlike the traditional sensors, in the remote sensor network, a vast numbers of sensors are densely deployed. These sensor nodes will perform significant signal processing, computation, and network self-configuration to .

ARCHITECTURE:

LAYOUT OF WSN:



In a typical WSN we see following network components –

• Sensor motes (Field devices) – Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself. International Journal of Next-Generation Networks

• Gateway or Access points – A Gateway enables communication between Host application and field devices.

• Network manager – A Network Manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network.

• Security manager – The Security Manager is responsible for the generation, storage, and management of keys.

USES OF BENEFIT: Buildings automation for controlling lights, fire alarms or access control, refrigeration control

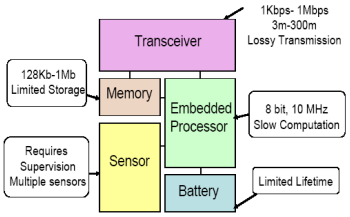
- Industrial automation
- Habitat monitoring
- Medical field
- Military

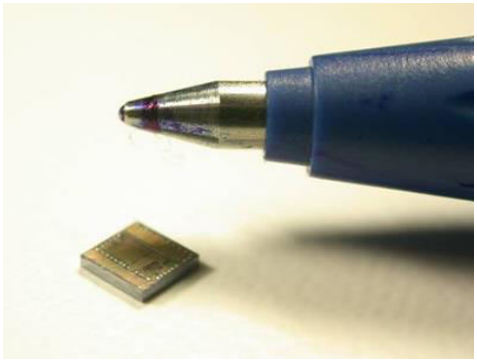
V.Swathy, J.Nisha Mary Gracea, s.shobana.

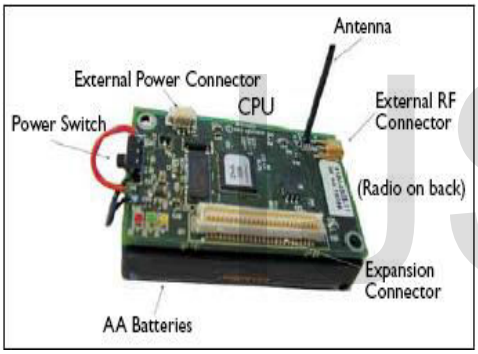
Department of MCA, GTEC, kanniyambadi, Vellore.

Sweetswathy1996@gmail.com

Nishaamalraj22@gmail.com







REQUIREMENTS OF WSN:

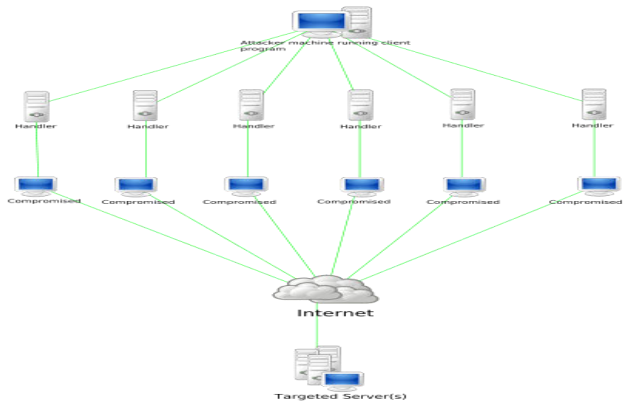
- Small in size and low power consumption
- Concurrency–intensive operation
- Concurrency–intensive operation
- Low cost
- Securit!

WSN SECURITY ANALYSIS: Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bits in the channel, replay previously heard packets and many more. Securing the Wireless Sensor Network needs to make the network support all security properties: confidentiality, integrity, authenticity and availability. Attackers may deploy a few malicious nodes with similar hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. Sensor nodes may not be tamper resistant and if an adversary compromises a node, she can extract all key material, data, and code stored on that node. While tamper resistance might be a viable defense for physical node compromise for some networks, we do not see it as a general purpose solution. Extremely effective tamper resistance tends to add significant per-unit cost, and sensor nodes are intended to be very inexpensive.

SECURITY THREATS:

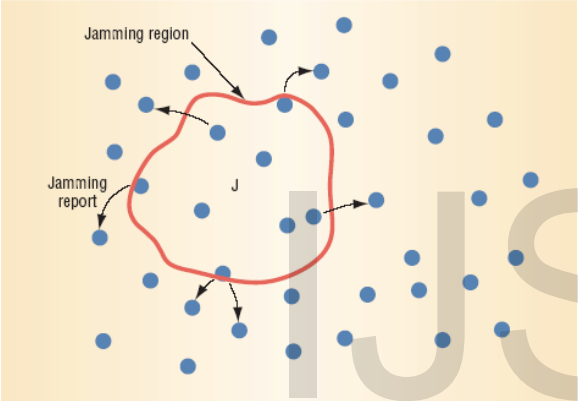
- Denial of Service.
- Spoofed, altered, or replayed routing info.
- Selective forwarding.
- Sinkhole attacks.
- Sybil attacks.
- Wormhole attacks.
- Hello flood attacks.
- Acknowledgement spoofing.

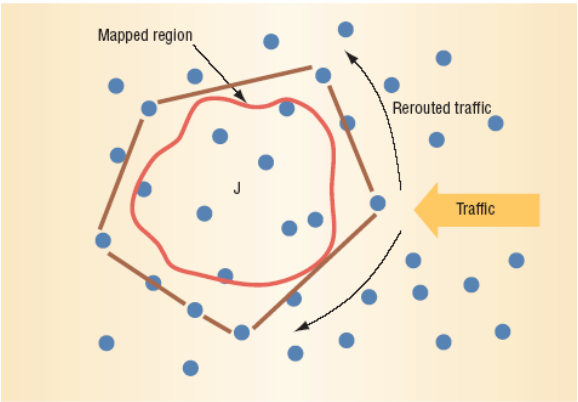
DENAIL OF SERVICE: In computing, a **denial-of-service attack** (**DoS attack**) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.[1] A DoS attack is analogous to a group of people crowding the entry door or gate to a shop or business, and not letting legitimate parties enter into the shop or business, disrupting no rmal operations.



Network Layer	DoS Attack	Defenses
Physical	Jamming	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode change
	Tampering	Tamper-proofing, hiding

DEFENSE AGAINST JAMMING:





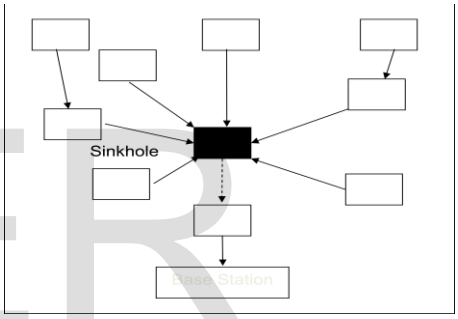
Spoofed, Altered, or Replayed Routing Info:

- Issues:
  - Routing info altered/falsified to attract/repel traffic from nodes.
  - Malicious nodes can create traffic loops.
- Counter Measures: Authentication.

Selective Forwarding:

- Issues:
  - Relies on routing methodology.
  - Subvert a node on a major traffic path.
  - Selectively forward only some data.
- Counter Measures:
  - Redundant routes.
  - Redundant messages.

Sinkhole Attack:



- Issues:
  - Subverted nodes close to base advertise attractive routing information.
  - Force nodes in the region to route data towards it.
  - Creates a 'sphere of influence'.
- Counter Measures:
  - Hierarchical routing.
  - Geographic routing.

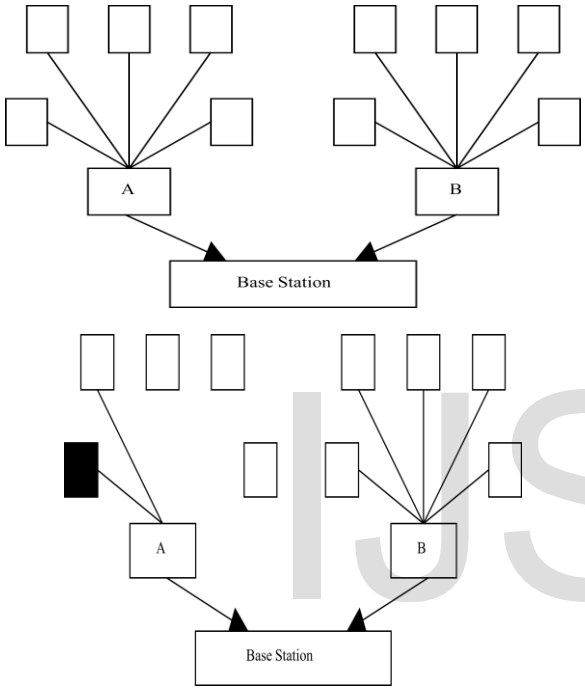
Sybil Attack:

- An adversary node assumes identity of multiple nodes.
- This causes ineffectiveness in a network. Specially target for networks with:

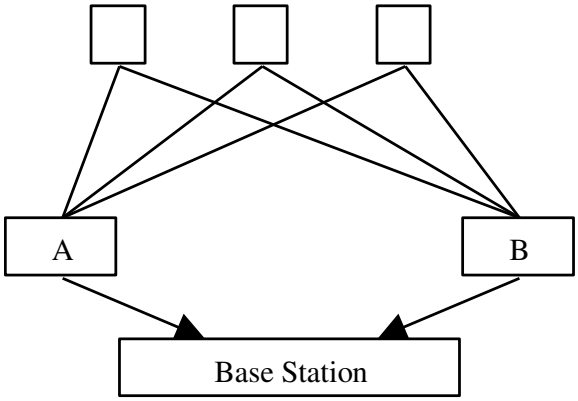
- Fault Tolerance
- Geographic routing protocol

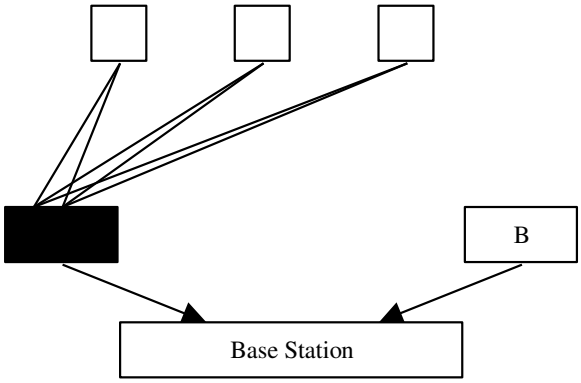
Sybil Attack (cont.):

- Geographic routing network where each intermediate node is allowed up to five connected nodes.
- Here, an adversary node assumes the identity of two nodes, leaving one node starved.



- In a network with fault tolerance, each node sends data to multiple intermediate node.
- Adversary intermediate node assumes multiple identity, removing the fault tolerance requirement.

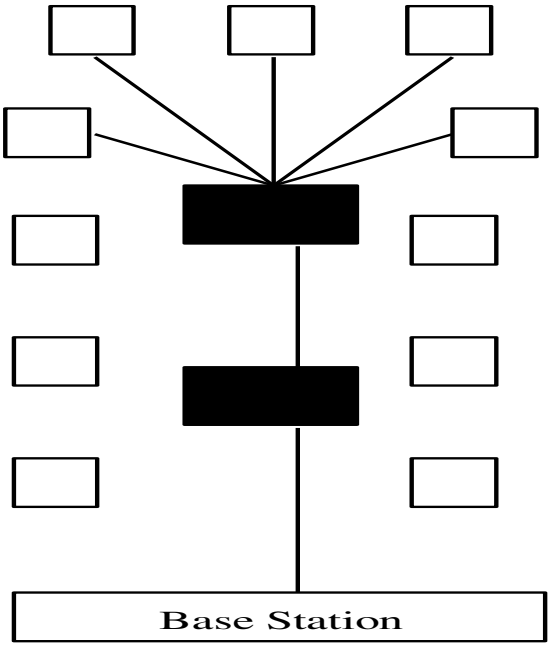




- Counter measure
  - Each node is assigned one or more "verified neighbors"
  - Traffic can go through verified or non-verified nodes.
  - Base station keeps track of how many neighbors each node has, and if the number is higher than normal, this indicates Sybil attack.
  - At this point, traffic can only be routed through verified nodes.
  - Neighbor verification can be done through certificates or public key cryptosystem.

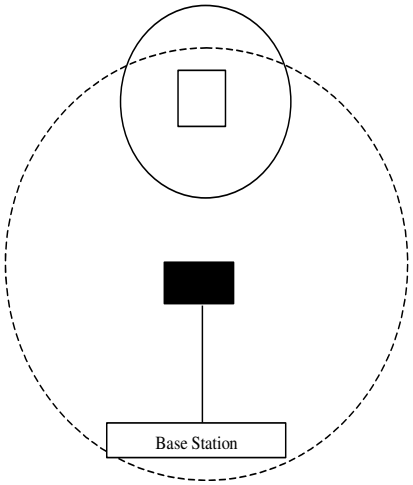
Wormhole Attack:

- Two powerful adversary nodes placed in two strategic location
- Advertise a low cost path to the sink
- All nodes in the network are attracted to them looking for an optimal route
- This is attack is usually applied in conjunction with selective forwarding or eavesdropping attack.
- The two adversary nodes advertise a route that's two hops away.
- Normal route is longer, so it's not used.
- The adversaries are now in control of all the traffic in the network.



HELLO flood attack:

- New sensor node broadcasts "Hello" to find its neighbors.
- Also broadcast its route to the base station. Other nodes may choose to route data through this new node if the path is shorter.
- Adversary node broadcast a short path to the base station using a high power transmission.
- Target nodes attempt to reply, but the adversary node is out of range.
- This attack puts the network in a state of confusion.
- nodes reply with randomly generated message.
- The new node must resend the messageCounter this attack by using a three-way handshake.
- New node sends HELLO.
- Any receiving back to the receiving nodes.
- This guarantees the bi-directionality of the link.

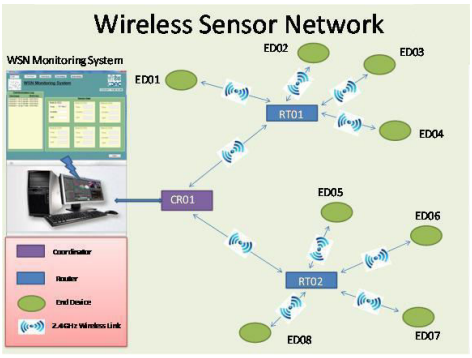


Acknowledgement Spoofing:

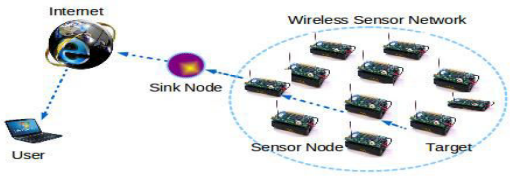
- Adversary can easily intercept messages between two parties
- Spoofs an acknowledge of a message to the sender.
- Goal is to convince the sender that a weak link is strong, or a dead link is still active.
- Counter the attack by appending a random number to the message and encrypt the whole thing. Acknowledge by sending the decrypted random number. \

WSN SYSTEMS:

WNS:



NETWORKS OF NETWORKS:



CONCLUSION:

- Wireless sensor network is a growing field and has many different applications.
- Most security threats to wireless ad-hoc network are applicable to wireless sensor network.
- These threats are further complicated by the physical limitations of sensor nodes.
- Some of these threats can be countered by encryption, data integrity and authentication.

  Security of wireless sensor network remains an intensive studied field

REFERENCES

[1] S. Sharma, "Energy-efficient Secure Routing in Wireless Sensor Networks", Dept of Computer Science and Engineering, National Institute of Technology Rourkela, Rourkela, Orissa, 769 008, India, 2009.

[2] D. Boyle, T. Newe,"Securing Wireless Sensor Networks: Security Architectures", Journal of Networks, 2008,

[3]. International Journal of Next-Generation Networks (IJNGN),Vol.1, No.1, December 2009 10 [3] X. Du, H. Chen, "Security in Wireless Sensor Networks", IEEE Wireless Communications, 2008.

[4] J. Granjal, R. Silva, J. Silva, "Security in Wireless Sensor Networks", CISUC UC, 2008.

[5] Y. Zou, K. Chakrabarty, "Sensor deployment and target localization based on virtual forces", INFOCOM 2003. Twenty- Second Annual Joint Conference of the IEEE Computer and Communications Societies. IEEE, Volume: 2, Pages: 1293 - 1303, April 2003.

[6] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", University of California at Berkeley.

[7] J. R. Douceur, "The Sybil Attack," in 1st International Workshop on Peer-to-Peer Systems (IPTPS '02), March 2002.

[8] Castro and Liskov, "Practical byzantine fault tolerance," in OSDI: Symposium on Operating Systems Design and Implementation. USENIX Association, Co-sponsored by IEEE TCOS and ACM SIGOPS, 1999.

[9] A. Banerjea, "A taxonomy of dispersity routing schemes for fault tolerant real-time channels," in Proceedings of ECMAST, vol. 26, May 1996, pp.129-148.

[10] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Wormhole detection in wireless ad hoc networks," Department of Computer Science, Rice University, Tech. Rep. TR01-384, June 2002.

[11] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly-resilient, energy-efficient multipath routing in wireless sensor networks," Mobile Computing and Communications Review, vol. 4, no. 5, October 2001. [12] A. Perrig, R. Szewczyk, V.Wen, D. Culler, and J. Tygar, "SPINS: Security protocols for sensor networks," in Proceedings of Mobile Networking and Computing 2001, 2001. [

13] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," Wireless Networks, vol. 8, no. 2-3, pp. 169-185, 2002.

[14] M.-J. Lin, K. Marzullo, and S. Masini, "Gossip versus deterministic flooding: Low message overhead and high reliability for broadcasting on small networks, Tech. Rep. CS1999-0637, 18, 1999.

[15] L. Li, J. Halpern, and Z. Haas, "Gossip-based ad hoc routing," in IEEE Infocom 2002, 2002. [16] Mona Sharifnejad, Mohsen Shari, Mansoureh Ghiasabadi and Sareh Beheshti, A Survey on Wireless Sensor Networks Security, SETIT 2007.