Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 5, May 2015, pg.182 – 191

RESEARCH ARTICLE

A Time Slot based Parametric Table Mapping Approach for Wormhole Detection in WSN

Deepika
Research Scholar, Department of Computer Science and Engineering, Ganga Institute Of Technology & Management, Kablana
Email ID: deepansi13@@gmail.com

Dr. Yashpal Singh
Asst. Professor (CSE Dept.) Ganga Institute Of Technology & Management, Kablana
Email ID: yashpalsingh009@gmail.com

Prof. S. Niranjan
Professor (CSE Dept.) Ganga Institute Of Technology & Management, Kablana
Email ID: niranjan.hig41@gmail.com

ABSTRACT:

A wireless sensor network is a combination of distributed sensor nodes that monitor physical or environmental conditions like as temperature, sound, pressure, etc. and send data through the network to a main location. WSN is also called infrastructure-based wireless network. In wireless sensor network ad-hoc infrastructure provide a bridge between the real physical and virtual worlds. It is provide to observe the previously unobservable at a fine resolution over large spatiotemporal scales. Ad-hoc topologies are provided support for detection and monitoring applications. A large number of nodes are with a dynamically changing membership. Wireless sensor nodes are called motes. WSN is a self-configuring network of small nodes communicating among themselves using radio signals, and deployed quantity to sense, monitor and understand the physical world. Sensor network node contains several parts like as a radio transceiver with an internal antenna, a microcontroller, usually a battery or an embedded form of energy harvesting. WSNs can be very from a simple star network to an advanced multi-hop wireless mesh network.

1. INTRODUCTION

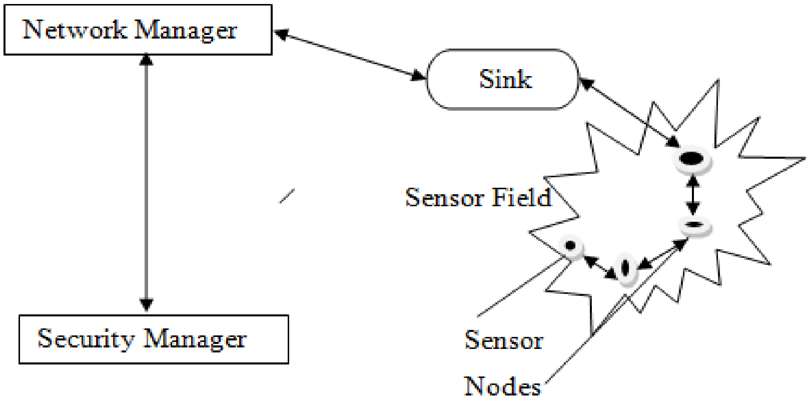
WSN Design

Sensor nodes:-A sensor node in a WSN that is capable of performing some processing, gathering information and communicating with other connected nodes in the network.

Sink:-It is provides communication between host application and field devices.

Network Manager:-It is provides for configuration of the network, scheduling communication between devices, create routing tables and monitoring health of the network.

Security Manager:-Like as task manager is responsible for the generation, storage and management of keys.



Sensor Node Design

Sensor node consist of transceiver, micro-controller, external memory, sensor1, ADC, sensor2 as shown in figure2 in which node is divided into six major blocks where each block perform some specific task.

Controller:-It performs tasks, processes data and controls the functionality of other components in the sensor node. Controller is a micro-controller, desktop microprocessor, digital signal processors, FPGAs, ASICs. Microcontroller is used in sensor nodes because of its low cost, provide flexibility, and low power consumption.

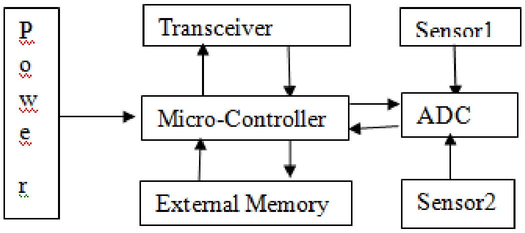
Transceiver:-Sensor node uses of ISM band which gives free radio, spectrum allocation, and global availability. Wireless transmission media means that radio frequency, optical communication and infrared. Transceivers are combination of both transmitter and receiver. The operational states are transmission, receive, idle, and sleep.

External Memory:-Memory needs are dependent on application. Two types memory used for storage are: user memory used for personal data, and program memory used for programming the device.

Power source:-The sensor node consumes power for sensing, communicating and data processing. So we need power storage like as batteries or capacitors. Two types of batteries rechargeable and non-rechargeable are used as main source of power supply for sensor nodes.

Sensors:-Sensors are hardware devices that measurable response to a change in a physical condition like temperature or pressure and monitored parameter of physical data. Wireless sensor nodes are very small electronic devices, consume low energy, and equipped with limited power source of less than 0.5-2 ampere-hour and 1.2-3.7 volts.

Three types of sensor like as: passive, Omni-directional, narrow-beam sensors and active sensor. WSNs are works with passive, Omni-directional sensors. Spatial density of sensor nodes in the field may be as high as 20 nodes per cubic meter.



2. CHARACTERISTICS

Scalability:-Scalability means that large scale of deployment. A sensor networks are combination of thousands, or more, micro-sensor nodes. So Scalability in sensor network protocols is an important requirement. Because every sensor nodes not containing global information about the network.

Low Complexity:-Sensor nodes are usually highly limited due to limitations from energy resource and cost. For this we need fully distributed, light weight localization one tracking algorithm is needed.

Ad-hoc Network:-Ad-hoc deployment implies no maintenance or battery replacement. To increase network lifetime no raw data is transmitted. Large numbers of self-organizing static as mobile nodes are possibly randomly deployed. Interference is high for Omni-directional antennas.

Lifetime: - Increase lifetime of network nodes is battery-powered. Nobody is going to change the batteries so save energy.

Simple: - WSN is a simple mobility of nodes. Distributed sensing as large no, of nodes are used to collect and storing data. Distributed sensing was provided robustness to the system. No need to install extra infra-structure for communication.

3. SECURITY

Wireless sensor nodes network means that shares common property as computer network. So we need security issues: - **Attack and Attacker**: **-** Attack means that unauthorized person access to a service. For security we need secure resource or information we need integrity, availability, or confidentiality of a system. Attackers can create fault and weakness in a security design, implementation, configuration or limitation are occurs.

Authentication:-WSNs transfer information and sensitive data for different important decision making. Receiver wants to the data with ensure that are correct source for decision-making process [10]. Authentication provides proof to sender node and receiver that data is secure in which they want to communicate.

Integrity:-Integrity means ensure that there must no tampering and extra data. Receiver check that data received is exactly original and same as send by the sender. Data integrity is to ensure that information is same during transmission by using some security key for ensure.

Confidentiality:-It gives guarantee that data send by the sender will not access by attacker. Encryption key is used for sending the message. Confidentiality means create security from unauthorized parties and attacker.

Scalability*:*-Scalability means that no node compromise and no increase communication when size of network is grow. It should allow nodes to be added in network with proper deployment as well.

Self-Organization:- In WSN Every sensor node is in dependent and flexible enough to be self organizing in different environments. No fixed infrastructure is available for WSN Network management. In self organizing we used conduct key management. In self organization we used conduct key management and building trust relation among sensor for security.

4. APPLICATIONS

Area Monitoring*:*- Area monitoring is a common application of WSNs area monitoring means that deployed over region in which phenomenon is to be monitored.

Forest Fire Detection*:*-We used network sensor nodes in a forest to detect when a fire has started. Sensor nodes work to measure temperature, humidity and gases which are produced by fire in the tree. After measurement easily apply action to control fire.

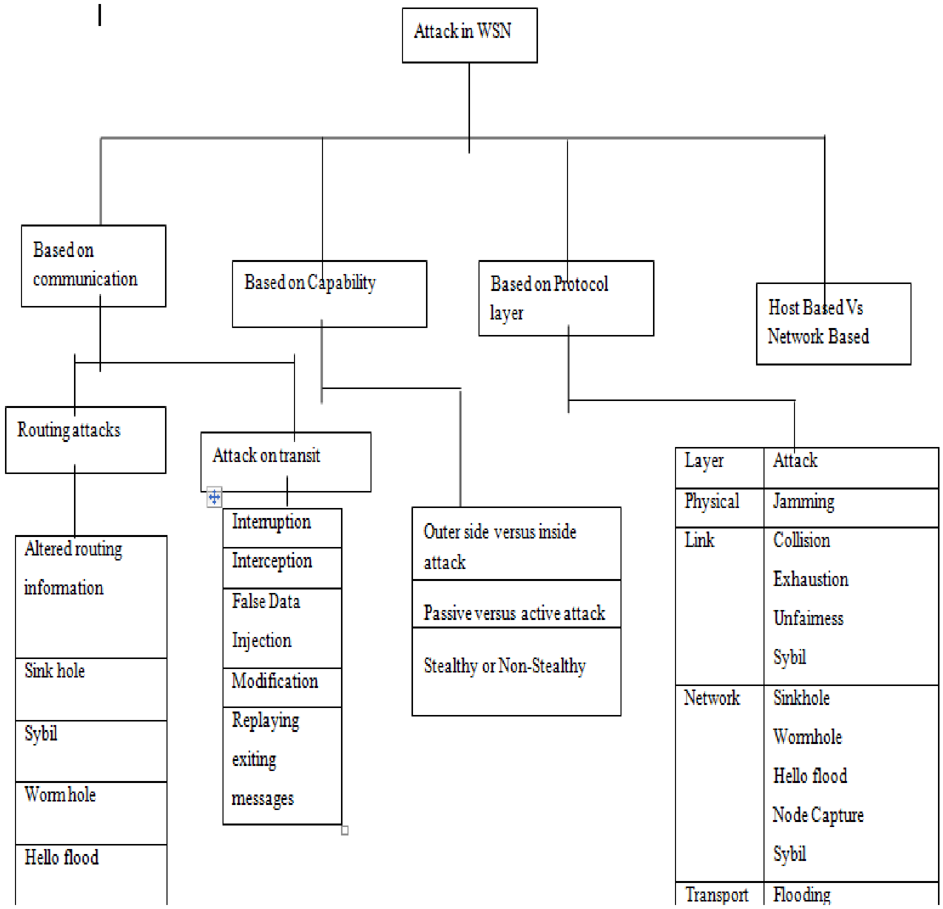
Industrial Monitoring*:*-Wireless sensor network have been developed for machinery condition-based maintenance as they offer significant cost savings and enable new functionalities. Wireless sensors provide low cost wiring for inaccessible locations, rotating, machinery, restricted areas and mobile assets.

Agriculture: -Wireless Sensor network is also widely used in agriculture these sensor are used to collect spatial data which act as information for farmers. In spatial data for crop management is through wireless sensor. This system can handle local field, surveys, and collect data of soil water availability, biomass yield, soil compaction, soil fertility, leaf area index, leaf temperature, local climate data, plant water status, and yield of grain etc.

Health Application:-Sensor networks are also widely used in health care areas. Many modern hospitals uses senor network to monitor patient physiological data, sensor networks are constructed to control the drug administration track and monitor the patients. E.g. pressure sensor, orientation sensor and sensors for detection of muscle activity etc. Intel deployed a 130-node network to monitor the activity of residents in an elder care facility. Patient data is acquired with wearable sensing nodes (“the watch”).

5. ATTACKS IN WSN

In wireless sensor network nodes are present on hostile or dangerous environment at that environment they are not physical protected. Attack and Attackers are means that unauthorized process that disturb the security service. A various types of attacks are possible in Wireless Sensor Network (WSN). Security attacks in WSN and all other networks can be roughly classified by the following criteria: Based on the Capability of the attacker, Attack on information in transit, Host based Vs Network based, Based on protocol layer, Attack on communication, Stealthy or Non-Stealthy.



Layer	Attack
Physical	Jamming
Link	Collision Exhaustion Unfairness Sybil
Network	Sinkhole Wormhole Hello flood Node Capture Sybil
Transport	Flooding

6. WORMHOLEATTACK

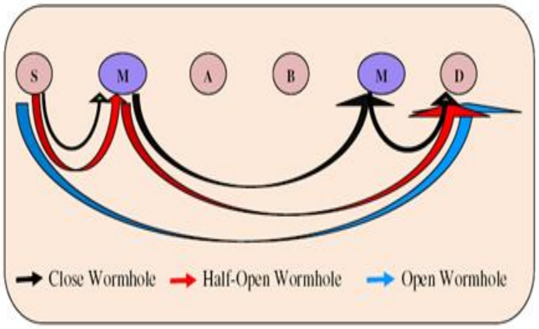
Wormhole attack like as a denial of service attack that disturb the network communication infrastructure without knowledge of the cryptography key methods. In wormhole attack may be created by a single or a pair of collaborating nodes in which two or more attackers are connecting by high speed off-channel link called wormhole link. A wormhole attack could be launched in two different modes: hidden and participation mode. In wormhole attack modes are depending upon attackers add their identity into packet headers when tunneling and replaying messages. In hidden mode attackers are not seen by the legitimate nodes. In this mode attackers put him on powerful position and during transmission capture message at one end of the wormhole and replicate them at the another end. This mode not need information about the authentication and encryption because its purpose only disturb and confused routing mechanisms. In this way it can create a virtual link between two far-off nodes by for example “tunneling“ the hello messages. So that hidden-mode wormhole attack is more difficult to defend against it. In participation mode attackers acquire valid cryptographic keys to attack on legitimate nodes. In this mode an attacker no need to create virtual link between the legitimate nodes. But they participate in the routing as legitimate node and use the wormhole to modify the original packet. This mode also very difficult to detect since the malicious nodes can simply ignore the security mechanisms of routing protocol.

Wormhole Attack Model:-Wormhole attack is a network layer attack (like as DoS) that can affect the network communication infrastructure without the knowledge of cryptographic techniques implemented. This is the reason why it is very difficult to detect. It is bombard by one, two or more number of nodes. In wormhole link it can create two ended wormhole, one end tunnels the packets and other end on receiving packets, replays them to local area. According to modes wormhole attack is classified into three models of wormhole attack like as closed, half open and open.

Open Wormhole:-Source and destination nodes and wormhole ends W_1 and W_2 are visible. Identities of nodes A and B, on traversed path are kept hidden.

Half-Open Wormhole:-First end of wormhole link node W_1 near the source is visible, while second end W_2 is set hidden. This leads to path S-W_1-D for message send by S for D.

Close Wormhole:-Identities of all the intermediate nodes ($W_{1,}$ A, B, W_2) on path from S to D are kept hidden. In this scheme both source and destination likes them just one-hop away from each other. Thus false neighbors are created.



7. TYPES OF WORMHOLE ATTACK

Number of nodes involved in establishing wormhole and the way to establish it classifies wormhole into following types.

Wormhole using Packet Encapsulation:- In encapsulation-based wormhole attack, several nodes exist between two malicious nodes and data packets are encapsulated between the malicious nodes. Only encapsulated packet message transfer no hop count incrementing. Here several nodes exist between two malicious nodes and data packets are encapsulated between the malicious nodes. Hence it prevents nodes on way from incrementing hop counts. The packet is converted into original form by the second end point. This mode of wormhole attack is not difficult to launch since the two ends of wormhole do not need to have any cryptographic information, or special requirement such as high-power source or high bandwidth channel.

Wormhole using Out-of-Band Channel:- In this attacker create out-of-band with high bandwidth channel in between two-end points in wormhole link. This kind of wormhole link only used one malicious node with high transmission capability in the network that attracts transmission of the intermediates node path that is passing from it. This mode of attack is more difficult to launch than the packet encapsulation method since it needs specialized hardware capability. Consider the outline presented in fig.. In wireless sensor network W_1 and W_2 are malicious nodes and they have an out-of-bound channel between themselves. Let us assume that source node (S) sends a RREQ to sink node and nodes A and W_1 are neighbors of S. Node W_1 transfer the RREQ to W_2 and W_2 broadcasts the message to its neighbors, including the sink node.

Sink node receives two RREQs: (S-W_1-W_2-Sink) and (S-A-B-C-Sink), sink node choose the first route because first route is faster and shorter than second than first route create out-of-bound modes of attack.

Wormhole using Packet Relay:-One or more malicious nodes can launch packet-relay-based wormhole attacks. In this type of attack malicious node replays data packets between two far nodes and this way fake neighbours are created. This kind of attack is also called as “replay-based attack” in the literature.

Wormhole using Protocol Distortion:-In this mode of wormhole attack, single malicious node tries to attract network traffic by distorting the routing protocol. This mode does not affect the network routing much and hence is harmless. Also it is known as “rushing attack” in the literature.

8. PROBLEM STATEMENT

According to survey large number of wormhole detection technique proposed but no anyone technique give a proper solution. Different problem like as:-

In Graphical and Topological Information based approaches:-

1.Need synchronized clocks

2.Need directional antennas and special hardware

In Location Information based method*:*-

1.Need directional antennas and special hardware

2. need geographical information

In Connectivity and Neighbourhood based approaches:-

1.Not present legal connectivity

2.Run extra search procedure and special hardware

In Message travelling time information based method:-

1.Need synchronized clocks

2.Need directional antennas and special hardware

In Graph theory method and Radio-fingerprinting:-

1.Need guard nodes

2.Require fingerprinting

3.433MHz radio signal

4.Only valid for one hop neighbour

9. TECHNOLOGY USED

OMNeT++ is an object-oriented modular discrete event network simulator. The simulator can be used for:
- traffic modeling of telecommunication networks
- protocol modeling
- modeling queueing networks
- modeling multiprocessors and other distributed hardware systems
- validating hardware architectures
- evaluating performance aspects of complex software systems
- . . . modeling any other system where the discrete event approach is suitable.

An OMNeT++ model consists of hierarchically nested modules. The depth of module nesting is not limited, which allows the user to reflect the logical structure of the actual system in the model structure. Modules communicate through message passing. Messages can contain arbitrarily complex data structures. Modules can send messages either directly to their destination or along a predefined path, through gates and connections. Modules can have their own parameters. Parameters can be used to customize module behavior and to parameterize the model's topology. Modules at the lowest level of the module hierarchy encapsulate behavior. These modules are termed simple modules, and they are programmed in C++ using the simulation library. OMNeT++ simulations can feature varying user interfaces for different purposes: debugging, demonstration and batch execution. Advanced user interfaces make the inside of the model visible to the user, allow control over simulation execution and to intervene by changing variables/objects inside the model. This is very useful in the development/debugging phase of the simulation project. User interfaces also facilitate demonstration of how a model works. The simulator as well as user interfaces and tools are portable: they are known to work on Windows and on several Unix flavors, using various C++ compilers.

OMNeT++ also supports parallel distributed simulation. OMNeT++ can use several mechanisms for communication between partitions of a parallel distributed simulation, for example MPI or named pipes. The parallel simulation algorithm can easily be extended or new ones plugged in. Models do not need any special instrumentation to be run in parallel – it is just a matter of configuration.

10. CONCLUSION

The paper has defined a work on wormhole attack. Wormhole is a type of attack in which two attacker nodes creates a link call wormhole link and these nodes give an illusion that the selected path is the shortest path to get the destination. The paper has defined the basic method to recover from these types of attacks

REFERENCES

1. Dargie, W. and Poellabauer, C.,"Fundamentals of wireless sensor networks: theory and practice", John Wiley and Sons, 2010 , pp. 168–183.
2. Sohraby, K., Minoli, D., Znati, T. "Wireless sensor networks: technology, protocols, and applications", John Wiley and Sons, 2007 ISBN 978-0-471-74300-2, pp. 203–209.
3. Saurabh Singh, Dr. Harsh Kumar Verma."Security for Wireless Sensor Network", International Journal on Computer Science and Engineering (IJCSE).

4. Saurabh Singh,Dr. Harsh Kumar Verma "Security For Wireless Sensor Network",International Journal on Computer Science and Engineering (IJCSE).
5. Liang song,"A Cross-layer Architecture of Wireless Sensor Networks for Target Tracking".Liang Song, Member,IEEE and Dimirices Hatzinakos Senior Member,IEEE.
6. Ajay jangra et. Al, "Wireless sensor network(WSN) Architectural Design Issues and Challenges" (IJCSE) International journal on computer science and engineering.
7. Saurabh Singh Dr. Harsh Kumar Verma, "Security For Wireless Sensor Network" Saurabh Singh et al. / International Journal on Computer Science and Engineering (IJCSE).
8. L. M. Ni and P. K. McKinley, "A survey of wormhole routing techniques in direct networks," Computer, vol. 26, no. 2, pp. 62–76, 1993.
9. Chaudhari H.C. and Kadam L.U."Wireless Sensor Network Security Attack and Challenges",International Journal of Networking,2011,pp-04-16.
10. Dr.G.Padmavathi and Mrs D.Shanmugpriya," A Survey of Attacks, Security Mechanisms and Challendes in Wireless Sensor Networks",International Journal on Computer Science and Information Security,2009,Vol 4.No.1&2.
11. C.Karlof and D.Wagner," Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", in Elsevier's Ad-hoc Network Journal Special Issue on Sensor Network Application and Protocols, vol.1,issue.2-3,pp.293-315,September2003
12. Y. Hu, A. Perrig, and D.Johnson., "Packet Leashes: A Defense against wormhole attacks in wireless Ad Hoc Networks", Proceedings of INFOCOM, 2003.2003.
13. L. Hu and D. Evans. "Using directional antennas to prevent wormhole attacks", Proceedings of network and distributed system security symposium, pp. 131-41, Feb.2004.
14. I. Khalli, S. Begchi, and N. B. Shroff.,"LITEWORP: A lightweight countermeasures for the wormhole attack in multi-hop wireless networks," Proceedings of international conference on dependable systems and networks,pp.612-41,2005.
15. S. Ozdemir, M. Meghdadi, and I. Guler." A time and trust based wormhole detection algorithum for wirless sensor networks", in 3rd information security and cryptology conference, pp.139-4,2008.
16. R.Shokri, M.Poturalski, G.Ravot, P.Papadimitratos, and J.P.Hubaux," A practical secure neighbor verification protocol for wireless sensor network", ACM WiSec. 2009.
17. Majid Meghdadi, Suat Ozdemir and Inan Guler, "A survey of wormhole-based attacks and their countermeasures in wireless sensor networks", IETE Technical Review, vol 28,issue 2,mar-apr 2011.
18. Y. Xu, J. Ford, and F. S. Makedon," A Variation on Hop-counting for Geographic Routing" Embedded Networked Sensors, 2006. EmNetSIII. The third IEEE Workshop on, 2006.
19. W. Sharif and C. Leckie. ,"New Variants of Wormhole Attacks for Sensor Networks", In the proceeding of the Australian Telecommunication Networks and Applications Conference, Melbourne Austrila, December 2006, pp.288-292.

20. N. Song, L. Qian, and X. Li. ,"Wormhole Attacks Detections in Wireless Ad Hoc Networks: A Statistical Analysis Approach." In Proceeding of the 19th International Parallel and Distributed Processing Symposium (IPDPS'05)

21. Dezun Dong, Mo Li, Yunhao Liu, Xiangke Liao ," Connectivity-Based Wormhole Detection in Wireless Ad Hoc and Sensor Networks", Parallel and Distributed Systems, International Conference on , December 2009, pp. 72-79 .

22. B. Prasannajit, Anupama S. Venkatesh, K. Vindhykumari, S.R. Subhashini, G. Vinitha ," An Approach Towards Detection of Wormhole Attack in Sensor Networks", Integrated Intelligent Computing , August 2010, pp. 283-289.