IJERST

International Journal of Engineering Research and Science & Technology

ISSN : 2319-5991
Vol. 3, No. 4
November 2014

www.ijerst.com

Email: editorijerst@gmail.com or editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 3, No. 4, November 2014

Research Paper

ANALYZE AN EFFICIENT TECHNIQUE TO SECURE AND DETECT MASQUERADE ATTACKS IN WSN

Jaiveer[1] and Manupriya Dua[1]*

Corresponding Author:* ***Manupriya Dua* ✉ *jaikhatana@gmail.com*

The purpose of this Research work is to develop an improvement in security and detection technology of masquerade attack in Wireless Sensor Network. Security has become the forefront of network management and implementation. The challenge in the security issue is to find a well balanced situation between two of the most important requirements: the need of developing networks in order to sustain the evolving business opportunities and work level, and the need to protect classified, private and in some cases even strategic information. The application of an effective security policy is the most important step that an institution can take to protect its network. Networks have grown in both size and importance in a very short period of time. If the security is compromised, there could be serious consequences starting from theft of information, loss of privacy and reaching even bankruptcy of that institution. The types of potential threats to network are continuously evolving and must be at least theoretical known in order to fight them back, as the rise of wireless networks implies that the security solution become seamlessly integrated, more flexible. 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.

Keywords: Wireless sensor networks, Ad hoc networks, Sensor network security, Secure communication architecture

INTRODUCTION

Wireless Sensor Networks (WSN) consist of small devices—called sensor nodes—with RF radio, processor, memory, battery and sensor hardware. One can precisely monitor the environment with widespread deployment of these devices. Sensor nodes are resource constrained in terms of the RF radio range, processor speed, memory size and power. WSNs follow specific communication patterns. Apart from this, sensor nodes are generally stationary. The traffic rate is very low and traffic is periodic as well. There may be long idle periods

[1] CSE Department, CBS Group of Engg. & Technology, Fatehpuri, Jhajjar, Haryana.

during which sensor nodes turn off their radio to save energy consumed by idle listening.

WSNs are mostly unguarded. Hence capturing a node physically, altering its code and getting private information like cryptographic keys is easily possible for an attacker. Wireless medium is inherently broadcast in nature. This makes them vulnerable to attacks. These attacks can disrupt the operation of WSN and can even defeat the purpose of their deployment. An adversary can launch DoS attacks without much effort (e.g., even without cracking keys used for cryptography-based solutions). Masquerade attacks can be very dangerous because adversaries can launch other attacks and can still hide and project themselves as legitimate nodes. Therefore, masquerade detection mechanisms are necessary. To be practical for real life WSN deployments techniques for detecting masquerade attacks should be lightweight.

The masquerade attack is a class of attacks, in which a user of a system illegitimately poses as, or assumes the identity of another legitimate user. Identity theft in financial transaction systems is perhaps the best known example of this type of attack. Masquerade attacks are extremely serious, especially in the case of an insider who can cause considerable damage to an organization. The insider attack detection problem remains one of the more important research areas requiring new insights to mitigate against this threat.

MASQUERADE ATTACK

Masquerade attacks can occur in several different ways. In general terms, a masquerader may get access to a legitimate user's account either by stealing a victim's credentials, or through a break in and installation of a root kit or key logger. In either case, the user's identity is illegitimately acquired. Another perhaps more common case is laziness and misplaced trust by a user, such as the case when a user leaves his or her terminal or client open and logged in allowing any nearby co-worker to pose as a masquerader.

Applications of WSNs are quite numerous. For example, WSNs have profound effects on military and civil applications such as target field imaging, intrusion detection, weather monitoring, security and tactical surveillance, distributed computing, detecting ambient conditions such as temperature, movement, sound, light.

PROBLEM FORMULATION

The objective of this research work is to implement security and detection techniques for attacks in wireless sensor networks. There are light weighted detection and security techniques already been developed and gives improved results but still there are some problems which need to be improved.

So, currently I am working on "Issues in detecting and securing WSN from masquerade attacks" and next task is "Improvement in existing detection and security techniques".

Although many of existing detecting techniques look promising, there are still many challenges that need to be solved in sensor networks. This work basically focuses on the improvement of the security issues of WSN so efforts can be made for trying to make the WSN free from (masquerade) attacks and make the sensor network more secure.

Research Problem

WSNs are mostly unguarded. Hence capturing a node physically, altering its code and getting private information like cryptographic keys is easily possible for an attacker. Wireless medium is inherently broadcast in nature. This makes them vulnerable to attacks. These attacks can disrupt the operation of WSN and can even defeat the purpose of their deployment. An adversary can launch DoS attacks without much effort (e.g., even without cracking keys used for cryptography-based solutions). Masquerade attacks can be very dangerous because adversaries can launch other attacks and can still hide and project themselves as legitimate nodes. Therefore, masquerade detection mechanisms are necessary. To be practical for real life WSN deployments techniques for detecting masquerade attacks should be lightweight (Vijay Bhuse).

Most current WSN routing protocols assume that the wireless network in benign and every node in the network strictly follow the routing behavior and is willing to forward packets for other nodes. Most of these protocols cope well with the dynamically changing topology. However, they do not address the problems when misbehavior nodes are present in the network.

A commonly observed misbehavior is packet dropping. Practically, in a WSN, most devices have limited computing and battery power while packet forwarding consumes a lot of such resources. Thus some devices would not like to forward the packet for the benefit of others and they drop packets not destined to them. On the other hand, they still make use of other nodes to forward packets that they originate. These misbehaved or malicious nodes are very difficult to examine that whether the packet dropping is intentionally by malicious node or dropped due to link error. WSNs have many characteristics that make them very vulnerable to malicious attacks. These are:

1. A wireless channel is open to everyone. With a radio interface configured at the same frequency band, anyone can monitor or participate in communications. This provides a convenient way for attackers to break into WSNs.
2. Due to standard activity, Most routing protocols for WSNs are known publicly and do not include potential security considerations at the design stage. Therefore, attackers can easily launch attacks by exploiting security holes in those protocols.
3. Due to the complexity of the algorithms, the constrained resources make it very difficult to implement strong security algorithms on a sensor platform. To design such security protocols is not an easy task. A stronger security protocol costs more resources on sensor nodes, which can lead to the performance degradation of applications. In most cases, a trade-off must be made between security and performance. However, attackers can break weak security protocols easily.
4. A WSN is usually deployed in hostile areas without any fixed infrastructure. It is difficult to perform continuous surveillance after network deployment. Therefore, a WSN may face various attacks.

Defining Normal and Malicious Behavior of the Node

The vulnerabilities in WSN provide intruder a way to compromise legitimate nodes and make them malicious in nature. In this section, an attempt has been made to define a normal and malicious behavior of a node. First of all, normal behavior of a node is defined and then malicious behavior.

Normal Behavior: "When any operation is performed in wireless sensor network (for example-all the packets from source node (S) to destination node (D) is delivered) while maintaining the security principles (Confidentiality (C), Integrity (I), Availability (Av), Authenticity (Au) and Non-Repudiation (NR)), then it is called the normal behavior of a node" (Jangra *et al.,* 2010).

Malicious Behavior: "When a node breaches any of the security principles and is therefore under any attack. Such nodes exhibit one or more of the following behavior:

Packet Drop: Simply consumes or drops the packet and does not forward it.

Battery Drained: A malicious node can waste the battery by performing unnecessarily operations.

Buffer Overflow: A node under attack can fill the buffer with fake updates so that genuine updates cannot be stored further.

Bandwidth Consumption: Whenever a malicious node consumes the bandwidth so that no other legitimate node can use it.

Malicious Node Entering: A malicious node can enter in the network without authentication.

Stale Packets: This means to inject stale packets into the network to create confusion in the network.

Delay: Any malicious node can purposely delay the packet forward to it.

Link Break: This can result in restricting the two legitimate nodes from communicating if the malicious node is between them.

Message Tampering: A malicious node can tamper the content of the packets.

Denying from Sending Message: Any malicious node may deny from sending messages to other legitimate nodes.

Fake Routing: Whether there exists a path between nodes or not, a malicious node can send fake routes to the legitimate nodes in order to get the packets or to disturb the operations.

Node Not Available: An intruder can isolate the node from taking part in any operation so as to create delays when the source node chooses another alternative path.

Stealing Information: Information like the content, location, sequence number can be stolen by the malicious node to use it further for attack.

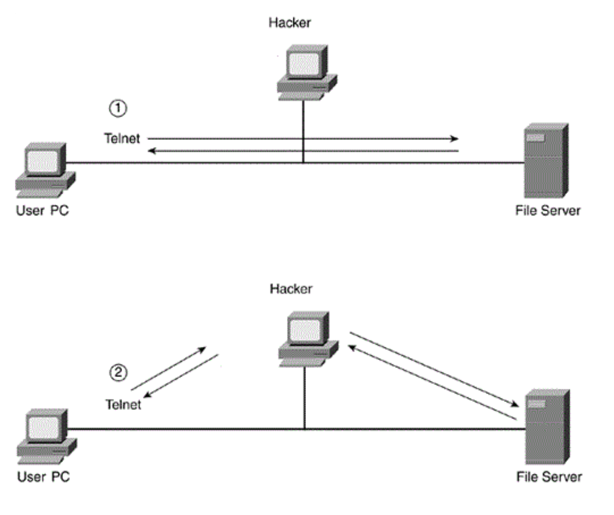
Session Capturing: When two legitimate nodes communicate, a malicious node can capture their session so as to take some meaningful information.

The problem, detection of the malicious nodes, has been addressed separately indifferent protocols, which are either extensions or based on secure routing protocols. There are various ways for providing security to networks. These are encryption, steganography, and securing access to the physical layer, etc.

Masquerade Attack in WSN

The masquerade attack is a class of attacks, in which a user of a system illegitimately poses as, or assumes the identity of another legitimate user. Identity theft in financial transaction systems is perhaps the best known example of this type of attack. Masquerade attacks (Figure 1) are extremely serious, especially in the case of an insider who can cause considerable damage to an organization. The insider attack detection problem remains one of the more important research areas requiring new insights to militate against this threat.

Figure 1: Masquerade Between User PC and File Server



A masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. The attempt may come from within an organization, for example, from an employee; or from an outside user through some connection to the public network. Weak authentication provides one of the easiest points of entry for a masquerade, since it makes it much easier for an attacker to gain access. Once the attacker has been authorized for entry, they may have full access to the organization's critical data, and (depending on the privilege level they pretend to have) may be able to modify and delete software and data, and make changes to network configuration and routing information (http://searchsecurity.techtarget.com/definition/masquerade).

User authentication is a crucial service in WSNs that is becoming increasingly common in WSNs because wireless sensor nodes are typically deployed in an unattended environment, leaving them open to possible hostile network attack. Because wireless sensor nodes are limited in computing power, data storage and communication capabilities, any user authentication protocol must be designed to operate efficiently in a resource constrained environment.

Security in WSNs

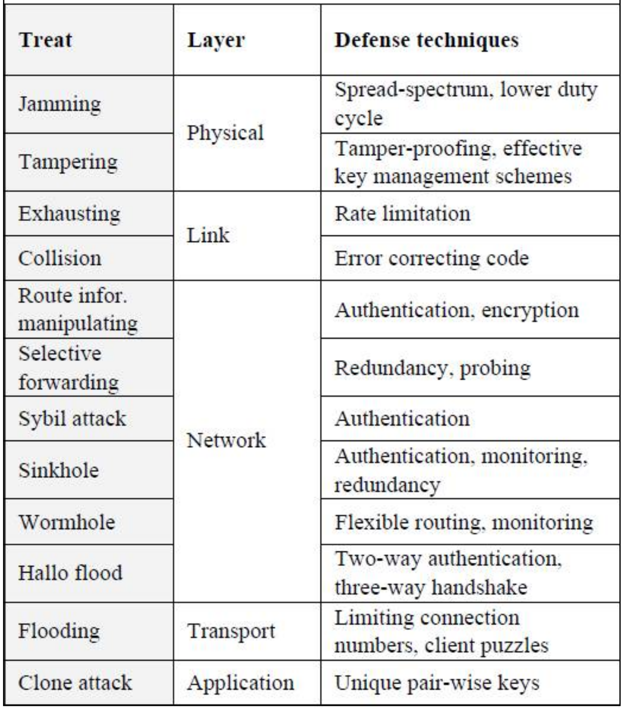
Due to inherent limitations in WSNs, security is a crucial issue and a sensor network is highly vulnerable against any external or internal attack, thus the infrastructure and protocols of the network must be prepared to manage these kinds of situations. This section examines the security problems that sensor networks face due to node resource limitations like memory and energy, sensor network constraints like unreliable communication, collisions and latency and physical limitation like unattended after deployment and remotely managed.

TYPES OF ATTACKS

Attacks on Sensor Network Routing: Many sensor network routing protocols are quite simple, and for this reason are sometimes susceptible to attacks from the literature on routing in ad-hoc networks. Most network layer attacks against sensor networks fall into one of the following categories:

- Selective forwarding
- Sinkhole attacks
- Sybil attacks

Table 1: Typical Treats in WSNs



Treat	Layer	Defense techniques
Jamming	Physical	Spread-spectrum, lower duty cycle
Tampering		Tamper-proofing, effective key management schemes
Exhausting	Link	Rate limitation
Collision		Error correcting code
Route infor. manipulating	Network	Authentication, encryption
Selective forwarding		Redundancy, probing
Sybil attack		Authentication
Sinkhole		Authentication, monitoring, redundancy
Wormhole		Flexible routing, monitoring
Hallo flood		Two-way authentication, three-way handshake
Flooding	Transport	Limiting connection numbers, client puzzles
Clone attack	Application	Unique pair-wise keys

- Wormholes
- HELLO flood attacks
- Acknowledgment spoofing

In the descriptions below, note the difference between attacks that try to manipulate user data directly and attacks that try to affect the underlying routing topology. Some general discussion of these types of attacks are given, how these attacks may be applied to compromise routing protocols that have been proposed.

Spoofed, Altered, or Replayed Routing Information

The most direct attack against a routing protocol is to target the routing information exchanged between nodes. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages, partition the network, increase end-to-end latency, etc.

DETECTION OF MALICIOUS NODE

Introduction

Any node under attack in wireless sensor network exhibits an anomalous behavior called the malicious behavior. Any malicious node in the network can disturb the whole processor can even stop it. To stop such malicious behavior several detection and prevention solutions have been discovered.

Existing Prevention Techniques

The most likely threats to public safety wireless deployments, especially those using 802.15.4 technologies, are passive eavesdropping, masquerading, and denial-of-service attacks. All of these are supported by widely available tools and can be difficult to detect. In addition, passive eavesdropping and denial-of-service can never be completely prevented.

1. Eavesdropping attacks are designed to expose protected information. Passive eavesdropping, the most likely eavesdropping threat, can be best prevented through the use of strong encryption against these attacks and are becoming widely available.
2. Masquerading attacks involve attackers inserting themselves into the wireless network. In most of these attacks, the attacker simulates the wireless access point itself. Fortunately, the Wireless Protected Access (WPA) and 802.11i technologies are effective defenses.

Wireless Protected Access

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are two security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.

WPA also includes a message integrity check. This is designed to prevent an attacker from capturing, altering and/or resending data packets. This replaces the Cyclic Redundancy Check (CRC) that was used by the WEP standard. CRC's main flaw was that it did not provide a sufficiently strong data integrity guarantee for the packets it handled (Communication in WSN). Well tested message authentication codes existed to solve these problems, but they required too much computation to be used on old network cards. WPA uses a message integrity check algorithm called Michael to verify the integrity of the packets. Michael is much stronger than a CRC, but not as strong as the algorithm used in WPA2. Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and the limitations of Michael to retrieve the key stream from short packets to use for re-injection and spoofing.

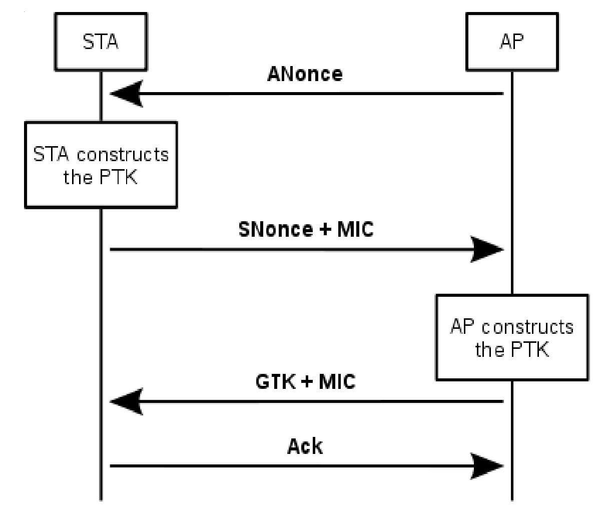
802.11i Technology

IEEE 802.11i, implemented as WPA2, is an amendment to the original IEEE 802.11.

Protocol Operation

IEEE 802.11i enhances IEEE 802.11-1999 by providing a Robust Security Network (RSN) with two new protocols, the 4-Way Handshake and the Group Key Handshake. These utilize the authentication services and port access control described in IEEE 802.1X to establish and change the appropriate cryptographic keys. The RSN is a security network that only allows the creation of Robust Security Network Associations (RSNAs), which are a type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Hand shake. It also provides two RSNA data confidentiality and integrity protocols, Temporal Key Integrity Protocol (TKIP) and Counter Mode Cipher Block (CCMP)

Figure 4: Actual Message Exchanged During the Handshake



The Four-Way Handshake

The authentication process leaves two considerations: the Access Point (AP) still needs to authenticate itself to the client station (STA), and keys to encrypt the traffic need to be derived. The earlier EAP exchange or WPA2-PSK has provided the shared secret key Pairwise Master Key (PMK). This key is, however, designed to last the entire session and should be exposed as little as possible. Therefore the four-way handshake is used to establish another key called the Pair wise Transient Key (PTK). The PTK is generated by concatenating the following attributes: PMK, APnonce (ANonce), STA nonce (SNonce), AP MAC address, and STA MAC address. The product is then put through PBKDF2-SHA1 as the cryptographic hash function.

The handshake also yields the Group Temporal Key (GTK), used to decrypt multicast and broadcast traffic. The actual messages exchanged during the handshake are depicted in Figure 4 and explained below:

1. The AP sends a nonce-value to the STA (ANonce). The client now has all the attributes to construct the PTK.
2. The STA sends its own nonce-value (SNonce) to the AP together with a Message Integrity Code (MIC), including authentication, which is really a Message Authentication and Integrity Code (MAIC).
3. The AP sends the GTK and a sequence number together with another MIC. This sequence number will be used in the next multicast or broadcast frame, so that the receiving STA can perform basic replay detection.
4. The STA sends a confirmation to the AP.

All the above messages are sent as EAPOL-Key frames.

As soon as the PTK is obtained it is divided into five separate keys:

PTK (Pairwise Transient Key – 64 bytes)

1. 16 bytes of EAPOL-Key Confirmation Key (KCK) – Used to compute MIC on WPA EAPOL Key message.
2. 16 bytes of EAPOL-Key Encryption Key (KEK) - AP uses this key to encrypt additional data sent (in the 'Key Data' field) to the client (for example, the RSN IE or the GTK).
3. 16 bytes of Temporal Key (TK) – Used to encrypt/decrypt Unicast data packets.
4. 8 bytes of Michael MIC Authenticator Tx Key – Used to compute MIC on unicast data packets transmitted by the AP.
5. 8 bytes of Michael MIC Authenticator Rx Key – Used to compute MIC on unicast data packets transmitted by the station.

The Michael MIC Authenticator Tx/Rx Keys provided in the handshake are only used if the network is using TKIP to encrypt the data.

The Group Key Handshake

The GTK used in the network may need to be updated due to the expiry of a preset timer. When a device leaves the network, the GTK also needs to be updated. This is to prevent the device from receiving any more multicast or broadcast messages from the AP.

To handle the updating, 802.11i defines a *Group Key Handshake* that consists of a two-way handshake:

1. The AP sends the new GTK to each STA in the network. The GTK is encrypted using the KEK assigned to that STA, and protects the data from tampering, by use of a MIC.
2. The STA acknowledges the new GTK and replies to the AP.

GTK (Groupwise Transient Key – 32 bytes)

1. 16 bytes of Group Temporal Encryption Key – Used to encrypt Multicast data packets.
2. 8 bytes of Michael MIC Authenticator Tx Key – Used to compute MIC on Multicast packet transmitted by AP.
3. 8 bytes of Michael MIC Authenticator Rx Key – This is currently not used as stations do not send multicast traffic.

Denial-of-Service (DoS) attacks can shut down a wireless network to some or all intended users or systems. DoS attacks are a common threat to all wireless technologies, but 802.11 networks are particularly vulnerable to these attacks. Although there are tools for detecting and triangulating the source of a DoS attack, there are no effective ways to prevent them, making these attacks virtually inevitable. Therefore, all public safety agencies should identify a backup communication mechanism to use in the event that the wireless network is unavailable.

PROPOSED PREVENTION TECHNIQUE

1. If link layer reports a link failure, try to repair the link locally using buffer information.
2. Remove the lost neighbor from all the precursor lists.
3. For each unreachable destination if precursor list non-empty add to RERR (route error) and delete the precursor list.
4. If a packet is forwarded where no route exist, drop the packet and send error upstream.
5. If a valid route has expired, purge all packets from send buffer and invalidate the route.
6. Check the TTL on every node, if it is zero, and then discard to prevent from routing loop.
7. Sequence numbers is used to determine an up-to-date path to a destination.
8. Set an expiry time to the route by adding active route time to current time.

CONCLUSION AND FUTURE SCOPE

Security is a significant issue in Wireless Sensor Networks. Intrusion of malicious nodes may cause serious impairment to the security. In the presented work, all the modes of AODV (simple mode and malicious node) have been discussed. This work can help in the area of security based systems.

In this dissertation work, AODV over WSN is simulated with different operation modes. An important contribution of this dissertation is the AODV with and without malicious node.

As the malicious node enters into the network, it tries to capture the network. The performance of the network is affected badly. The parameters measured are number of packet send, and number of packet received, packet delivery ratio and number of packet dropped. But, after detecting the malicious node, performance of the network increase. Malicious node drops the entire packet but IDS again increase the packet delivery ratio and decrease the packet drop rate.

In future work other parameters can also be considered like energy consumption, overload, throughput, etc. IDS is implemented on AODV protocol, other protocols like DSR, DSDV, FSR can be used. Malicious node can cause many other type of attacks except packet dropping like battery drained, stale packets, message tempering, node not available, fake routing, etc.

Practical WSN security is a balancing act that is constantly in search of the highest level of protection that can be done even in constraint of limited resources. A large number of security problems are still open in WSN. One of the open problems is authentication of sensor nodes. If there is proper authentication in the network, chances of entering malicious node is very less. To secure the sensor network when a new node enters into the network, it should be authenticated IDs,

REFERENCES

[1. About a Masquerade http://searchsecurity.techtarget.com/definition/masquerade

2. Akkaya K and Younis M (2004), "A survey

on Routing Protocols for Wireless Sensor Networks", *Computer Networks (Elsevier) Journal.*

3. Akyildiz I F and Su W and Sankara subramaniam Y and Cayirci E (2002), "Wireless sensor networks: a survey", *Computer Networks,* Vol. 38, pp. 393-422, March.

4. Applications of WSN : http://www.docstoc.com/docs/83212145/wsn-applications-challenges

5. Bhuse V and Gupta A (2006), "Anomaly intrusion detection in Wireless Sensor networks", *Journal of High Speed Networks,* Vol. 15, No. 1, pp. 33- 51.

6. Castro M and Liskov B (1999), "Practical byzantine fault tolerance", in: OSDI: Symposium on Operating Systems Design and Implementation, USENIX Association, Co-sponsored by IEEE TCOS and ACM SIGOPS.

8. Communication in WSN: http://enews.i2r.a-star.edu.sg/tech_wireless.htm

9. *Cygwin* http://en.wikipedia.org/wiki/Cygwin

10. Das S R and Castaneda R, Yan J and Sengupta R (1998), "Comparative performance evaluation of routing protocols for mobile, ad hoc networks", In 7th Int. Conf. on Computer Communications and Networks (IC3N), pp. 153-161, October.

11. Das S R, Castaeda R and Yan J (2000), "Simulation-based performance evaluation of routing protocols for mobile ad hoc networks", *Mobile Networks and Applications,* pp. 179-189.

12. Handy M J, Haase M and Timmermann D (2002), "Low Energy Adaptive Clustering Hierarchy with Deterministic Cluster-Head Selection", *IEEE MWCN.*

13. Ishida K and Kakuda Y, Kikuno T (1992), "A routing protocol for finding two node-disjoint paths in computer networks", in: *International Conference on Network Protocols,* pp. 340–347.

14. Jamal N Al-Karaki and Ahmed E Kamal (2004), "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Communications,* Vol. 11, pp. 6-28, Dec.

15. Jangra A Goel, Priyanka N and Bhati K (2010), "Security Aspects in Mobile Ad Hoc Networks (MANETs)" A Big Picture", *International Journal of Electronics Engineering,* pp. 189-196.

16. Jones K, Waada A, Olaniu S, Wison L and Eltoweissy M (2003), "Towards a new paradigm for Securing Wireless Sensor Networks", *New Security Paradigms workshop,* Ascona, Switzerland.

17. Malek Ben Salem and Salvatore J Stolfo (2009), "Masquerade Attack Detection Using a Search-Behavior Modeling Approach", Computer Science Department Columbia University New York, USA fmalek, salg@cs.columbia.edu

18. Vijay Bhuse, Ajay Gupta and Ala Al-Fuqaha (2007), "Detection of masquerade attacks on Wireless Sensor Networks" , Department of Computer Science, Western Michigan University, Kalamazoo, MI 49008 2 Institute of Security Technology Studies, Dartmouth College, Hanover, NH 03755.

19. Scott E Coull and Joel W Branch and Boleslaw K Szymanski and Eric A Breimer,

"Sequence Alignment for Masquerade Detection", Baltimore, MD 21202 Troy, NY 12180 Loudonville, NY 12211 (410) 516-8775 (518) 276-8326 (518) 786-5084

20. Security Goals ByP Fleege rhttp://www.cis.temple.edu/~jfiore/2012/spring/4378/handouts/pfleeger/ch01/ch01.pdf

21. Whitehouse K and Woo A, Jiang F, Polastre J and Culler D (2005), "Exploiting the Capture Effect for Collision Detection and Recovery", *The Second IEEE Workshop on Embedded Networked Sensors (EmNetS-II),* May.

22. Xu Y, Heidemann J and Estrin D (2001), "Geography-informed energy conservation for ad hoc routing," *in: Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking.*

23. Shakkottai S, Srikant R and Shroff N (2003), "Unreliable sensor grids: coverage, connectivity and diameter", INFOCOM 2003, *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies,* April .

24. Simulation http://en.wikipedia.org/wiki/Simulation.

International Journal of Engineering Research and Science & Technology
Hyderabad, INDIA. Ph: +91-09441351700, 09059645577
E-mail: editorijlerst@gmail.com or editor@ijerst.com
Website: www.ijerst.com

ISSN 2319-5991