ISSN 2229-5518

Security Challenges & Preventions in Wireless Communications

Kashif Laeeq

Abstract— Without the need of an infrastructure, low-cost, auto-managed, flexible and low power consumer, wireless communication is becoming emerging technology. It shows great binder for present as well as future hi-tech applications. Increasing reliance on wireless communication also brings great challenges to the security measures and other correlated issues. Although the newly introduced corrected security standard, IEEE 802.11i, offers extensive security for the wireless environment but it is still premature and does not provide effective measures to protect the wireless networks from confidentiality and integrity threats. The main issues for deployment of wireless networks are security attacks, vulnerabilities, battery power and improper security models. This paper provides a study on these problems especially in ad-hoc wireless networks. The study is based on numerous proposed schemes in the endeavor to secure such networks. The goal of this paper is to probe the principal security issues, challenges and fundamental security requirements of wireless communications on the bases of their proposed solutions.

Index Terms— Attack, Denial of service, Mobile Ad-hoc Networks, Security issues, Vulnerabilities, Wireless Communication, WSN.

1 INTRODUCTION

DUE to low cost, low power consumption, flexible, no physical infrastructure and easy to deploy, wireless communications have been an admired research area over the past few years with tremendous growth in the population of wireless users. Many systems are still mapping wire to wireless media. Nowadays , there are number of wireless technologies on hand for long range applications like cellular mobile, satellite communications, Radio Frequency (RF), and short range applications such as Bluetooth, Infrared (IR), Near Field Communication (NFC), ZigBee, Ultra Wide Band (UWB). These short range wireless technologies are being used in many wireless technologies like wireless local area networks (WLAN), wireless body area networks (WBANs), wireless personal area networks (WPANs), and, ad-hoc network etc. Although wireless communications have numerous compensations over the usual wired networks in contrast it is exposed to a range of intrusion attacks. Unlike the wired networks, the wireless networks face unique challenges due to their inherent vulnerabilities. Any wireless signal is subject to interception, jamming and false command disruption.

The coverage area of wireless communication is dependable on the devices used. The more powerful device may cover large area but it will be expensive, consume more power and also produce more electromagnetic radiation that might be danger for human health [11]. One of the solution provides in that enlarge the coverage area hop by hope, by applying the ZigBee protocol, but the energy issue remain constant. Majority of times the limited energy restrict the security schemes [15].

Nearly all the proposed solutions concentrate on a specific security problem but pay no attention to others, those which pull off low energy and memory burning up negotiates on security level. Therefore the demand for a model; which fulfills all these issues with low cost, high security and low power, is increasing with raising the wireless technology.

Attack, is also one of the major issues in wireless communications. The technology suffers with two major types of attacks, i.e. inside and outside attacks. Outside attacker can't get access to the network but inside attacker can do it and may disrupt the network resources such that encryption keys or further codes used by the network. It is observed many times that only cryptographic security schemes may be failed to combat with numerous types of attacks in contrast all the proposed intrusion detection systems are not surely detect and remove the intruders. In reactive routing protocols like AODV, chances of attack are higher [18].

2 ISSUES AND CHALLENGESS

Wireless communication has emerged as a major breakthrough in traditional wired communications. It has changed messy wired world into a clean and flexible atmosphere. According to a well known adage, *there is no unmixed good in this world*; implementation of wireless network carries numerous performance and security issues. These issues include:

2.1 Vulnerabilities in Current Wireless Communications

The wireless communications survivability relates to wireless communication protection mechanism and robustness against attacks and failure of wireless network elements or communication itself. Some of these issues are as follows:

• *Kashif Laeeq is lecturer at Computer Dept. in Federal Urdu University of Arts, Science & Technology, Karachi, Pakistan, PH-03002511667. E-mail: kashiflaeeq@yahoo.com*

- The Wireless Sensor Network gateway forms a single point of breakdown for the back-to-back sensor network infrastructure [1].
- After deployment of network, sensor nodes remain unattended which is a root cause of security lapses [2].
- The existing location tracking methods have their own boundaries in tracing wireless intruders [3].
- Major threat and challenges of wireless communications are still not considered in IEEE 802.11i revised specification [4]
- Ad-hoc Wireless Sensor Networks deployment for monitoring physical environments are still in vulnerable zone [5].

2.2 Current Security Models and Prevailing Security Threats

Different performance issues of wireless networks operation, administration and management are encountered due to improper security model. Many security schemes don't guard against some prevailing threats. Some of these issues are as follows:

- Present security schemes for Wireless Personal Area Networks (WPANs) are immature [6]
- There is no proper visualization technique present for wireless communications [7]
- Security model for wired network not necessarily effective for wireless networks [8].
- Compressed Real time Transport Protocol (CRTP) is not appropriate for wireless links, that have a very high and erratic bit error rate (BER)[9]
- Inadequate security integration scheme for heterogeneous networks [10].
- The current wireless smart home system has range limitation issue [11].

2.3 Major Attacks on Wireless Sensor Net works (WSN)

Wireless Sensor Network (WSN) is a prevailing technology that shows great promise for diverse ultramodern applications both for mass public and intelligence. Security in wireless sensor networks is still in its childhood, as little consideration has been made to this area by the research community, due to this ignorance, WSN still facing numerous issues and challenges. Some of these issues are as follows:

- There is no common model to guaranteed security for each layer in a Wireless Sensor Networks (WSNs) [12].
- Current security Solutions for wireless Sensor networks are not feasible against all Prevailing security threats [13]
- Protection mechanism in wireless sensor network is still adolescent age [14].
- The current protocols for data link layer & network layers are not adequate for handling various security threats in WSN [15].
- The existing security measures for wireless sensor networks (WSN) are insufficient [16].

2.4 Security Attacks on Ad-hoc Wireless Networks

Truly speaking the most demanding area of wireless networking is ad-hoc wireless networks, but unfortunately it is the most at risk. Any intruder can easily get the access on the network resources and disrupts the communications. Some of these issues are as follows:

- In many cases cryptographic-based solution for detection the intruder in ad-hoc networks are ineffective [17].
- Attacks on wireless ad hoc network specially on routing protocols upsets network performance and reliability [18]
- No response method and limitations to handle wormhole attacks in Wireless Ad-hoc Networks (WANs). [19].
- Many existing ad-hoc routing protocols concern only the length of the routers [20].

3 APPROACHES TO MITIGATE ABOVE CHALLENGES

The main issues for deployment of wireless networks are security attacks, vulnerabilities, battery power and improper security models. The research on security issues and challenges in wireless communication comprises performance implications due to different factors. The effects of these factors or problem areas have been addressed by using different tools, algorithms, models, simulations and design modifications. These sub domains and the approaches or methodologies are discussed in subsequent paragraphs:

3.1 Protecting Wireless Network against Vulnerabilities

The Wireless Sensor Network gateway forms a single point of collapse for the back-to-back sensor network infrastructure. Even if a strong security model is used, but whenever intruder attacks on WSN-gateway, the whole network operations hampered. The fault endurance of WSN-gateway should be increased to avoid single point failure. In [1] a commercial grade WSN is considered and threw a ping-based DDos attack on the gateway of WSN. Various computers send ping attack traffic simultaneously to the WSN-gateway. For the entire testing of 4 hours of DDoS attack, processor fatigue and sensed data were collected. It is clearly observed that the computing resources of network gateway exhaustion under ping-based DDoS attack traffic. At a load exceeds by 20% of the ping attack, the WSN gateway processor became 100% busy, which caused the WSN-gateway to discontinue collection, reporting and recording the log sensor data. Result of this experiment stress to increase the fault endurance to avoid

single point failure. [1].

Due to the vulnerable attributes of sensor networks, there is always a risk of threats, along with the objective to ensure the privacy, integrity and reliability of transmission over these sensor networks. Model present in [2] associated with Communal Reputation and Individual Trust (CRIT) within sensor nodes overcomes this problem. In this model, a node judge the reliability or adequacy of a neighbor node throughout a set of values associated to the neighbor node's reliability and reputation. A node observes their neighboring nodes and positions the neighbors in conditions of a trust vote. Trust table kept by neighboring nodes conclude the communal and individual trustworthiness of nodes. A node keeps two tables, a trust table and other is reputation table. Trust table keeps the trust and un-trust observations for all other neighbor nodes. In the same way reputation table keeps reputation observations for all the neighbor nodes. If a node throws a unique message, and that is not confirmed by all other nodes, then the reliability of the node is under question, and also the un-trust value for the node increases. This message comes to cluster leader, by all other nodes about a specific node, it transmit the information so that all other nodes disregard the untrustworthy node and it is discarded from the network [2].

The current location tracking schemes have their own boundaries in tracing wireless intruders. The modification for Triangulation method present in [3] seeks to overcome this limitation. The technique based on two separate databases, the values of these databases consider by two locations, one for inside and other for outside the building. For location tracking using databases, execute the Triangulation method followed by matching up to the value with entries of data bases. It will be at a glance that attacker is inside the building or outside, then looking for closest values in databases; the matching observations in column without having triangulation would be the more precise location of device [3].

The IEEE 802.11i modification has concluded to deal with security issues in wireless local area networks but major threats like DoS attacks, insider attacks and offline guessing attacks are still looked-for consideration. An improved authentication mechanism present in [4] can overcome this ignorance. This scheme adopts an asymmetric cryptography technique to achieve effective defense in six categories that are discovery phase, authentication and association phase, RADIUS authentication, 4-way handshake, group key handshake, and secure data communication. This integrated protection for, null data frames, EAPOL frames, management frames as well as protection from some fundamental DoS attacks, Offline guessing attacks and insider attacks. This authentication mechanism is also capable to allow stations to organize themselves automatically [4].

Ad-hoc wireless sensor networks deployment for monitoring physical environments, where targets have unforeseen motions, are still in vulnerable zone. For such type of Self Organizing Wireless Sensor Networks (SOWSNs), stat-mesh architecture and mobility scheme provide an efficient monitoring system [5]. The architecture has a base station (BS) node and sensor nodes (SN), which unites a mesh of routers to expand radio coverage with star endpoints. Star-Mesh architecture utilizes multi-hopping to offer multipath routing, by means of an ad-hoc network based approach. The SN collects environmental in formations and re-arranging events generated by BS. The BS performs actions on receiving events also managing the routes. Initially when a node gets a message it stores the flooded one and transmit the message to all its neighbors. A new received message that has the same flood id is erased. Each SN has an initial amount of power hence it can drive signals to all nodes surrounded by its transmission range. Each SN connected at least one B.S. the BS, with great amount of energy, works as a gateway that connects SN to the analysis center. The BSs are fixed and each BS knows exactly its position information. The BSs are assumed to be arbitrarily located. [5]

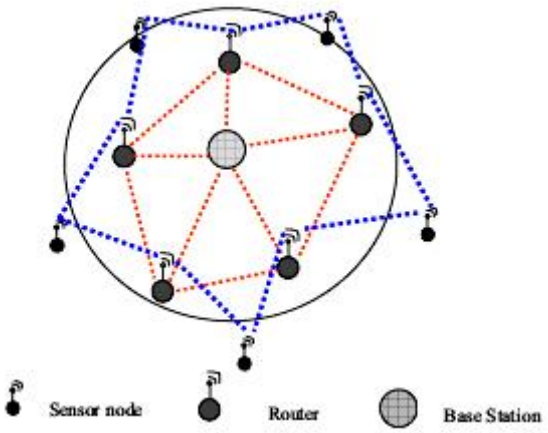

Fig.1: The Ad-hoc SOWSN architecture [5]

3.2 Schemes to Reduce Current Security Threats and Range Limitation Issues

At hand security schemes for Wireless Personal Area Networks (WPANs) needed more research. In [6] T.Kennedy and R. Hunt review WPAN security according to them protection mechanism for Bluetooth is that PIN should not entered into the Bluetooth devices for paring in public and only known devices should pair. Encryption technology is essential for unique session key. For ZigBee the source decides whether a protected or non-protected acknowledge frame is needed, also performing authentication of the source address. Use symmetric key key exchange (SKKE) acknowledgement of a link key between trust centre and connected devices. For Near Field Communication, a standard key handshake protocol such as diffie-Hellman associated on elliptic

curve cryptography, or RSA could be used to set up a shared secret between two devices for securing the channel [6].

Wireless network visualization techniques in presentation mode visualize the information of access points, mobile devices and relationship using the icons, colored lines and symbol. in this way more information about network status and performance can be achieve, and will help the network performance and security attacks [7].

A novel method using MAC Spoofing proposed in [8] used to avoid any intruder into the wireless communications. MAC address of authenticated user can be used to save any unauthorized access a data base of all authorized client MAC address maintain by organization. If the intrusion detection system finds more than one request of MAC address in the same network, it can be sure that the MAC address has been fraud and can block access to that MAC address temporarily [8].

A modified Enhance Compressed Real-time Transport Protocol (ECRTP) is suitable for wireless point-to-point links, which have a very high and erratic Bit Error Rate (BER). In modified ECRTP, the size of header is reduced. In compressed RTP packets occupy only 2 bytes. These bytes may be the UDP check-sum or the compressor interleaved header checksum. By sending these checksums only in some packets, the average header size can be reduced [9].

Heterogeneous Network Integration Model proposed in [10], yields a security scheme for wireless mesh networks. Each of the mixed wireless networks has produced connection with mesh backbone throughout the mesh gateway interface. Whenever these networks correspond with the mesh cloud, they cross the gateway routers of mesh backbone. Security issues of the border between the heterogeneous wireless networks and the mesh communications should be contracted intensively. In order with this, when passing during the mesh cloud, every of these heterogeneous networks require the mesh infrastructure to perform their own individual security requirements.

The current wireless home system has range limitation issue. By using IEEE 802.15.4 standard a system is proposed for smart home environment. The most vital part of the structure is main controller, which will provide interfacing between users and the system. PICI8f452 microcontroller is used as a brain of the main controller for low power consumption CMOS technology's ICs are used. A GSM modem is attached with the controller for SMS. Approximately nine phone numbers can be stored and only these numbers can communicate with main controller for sending & receiving SMS & system resource controller. User can enter into system by entering password. The software consists of programming PICI6LF452 microcontroller using Mikroc compiler from Mikroelectronika. Using C-Language, all of this programming is completed [11].

3.3 Preventive Measures against Security Issues in Wireless Sensor Networks

Majority of proposed security schemes are supported by particular network model. It is needed to have a model that accomplishes the need of security for each layer in a network. The proposed holistic approach [12] with respect to security for wireless sensor networks mitigates this issue. The holistic scheme has some fundamental principles like in a certain network; security is to be guaranteed for all the layers of protocol stack, the value for ensuring security should not exceed the assessed security risk at a particular time, if there is no substantial security ensured for the sensors. In a particular network; safety is to be ensured for every layers of the protocol stack then the cost for guarantee security should not exceed the assessed security risk at a particular time, if there is no physical security guaranteed for the sensors. The security evaluate must be capable to exhibit a refined degradation if some of sensors in the system are compromised. The security considered should be developed to function in a decentralized mode. If security is not measured for all the security layers there are a few efficient security methods working in other layers. By formation security layers as in the holistic scheme, protection could be recognized for the overall network [12].

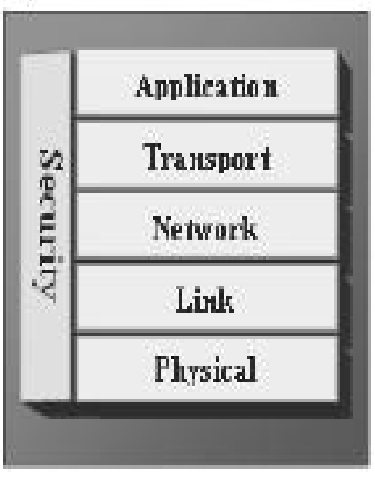

Fig.2: Holistic View of Security in wireless sensor networks [12]

Classification and association of security VTA (Vulnerabilities Threats & Attack), is proposed to remodel application-specific WSNs. The proposed scheme has redefined the concepts of vulnerability, threats and attacks with respect to wireless sensor network. On the basis of this differentiation we can check the list of security VTAs, which can reduce the ambiguity of security information on VTAs. Then; by probing each of VTAs we relate it with a security appraisal framework for analysis [13].

Table 1. Classification and Association of Security VTAs with Discrete Security Assessment Framework [13]

N E	Vulnerability: average energy exhaustion (network), low computational capacity, limited network storage time,

TWORK	self organization, fault-tolerance level, distributed storage, task details, simple ciphering, and node deployment
	Threat: Topology change, change of frequency, large messaging overhead, non-scalability, recursive routing, system failures
	Attack: complete DoS or DDoS
LINK	Vulnerability: Radio link, Signal transmission range (916MHz,2.4GHz), Broadcasting, Topology-less infrastructure, Ad hoc Topology information
	Threat: Non-Reachable, Link-failure, High-density of nodes, Indefinite jamming of signals, Data tampering, High noise, unmanaged mobility, Higher delays (link-setup)
	Attack: Collision or checksum mismatch, Unfairness, Spoofing, Sybil, Wormholes, Hello flood, ACK-spoofing
SINK	Vulnerability: Energy exhaustion at Sink, Task details
	Threat: Unauthorized access
	Attack: Sinkhole, de-synchronization
NODE	Vulnerability: Energy exhaustion at node, Resilience to physical security, Limited memory, short-storage time
	Threat: Node failure, Recursive localization, Indefinite flooding
	Attacks: Selective Forwarding
OTHER	Vulnerability:------
	Threat: Natural hazards, Environmental interference, Human Interaction (to damage network), catastrophic(man-made)
	Attack: Nil

Multitier security architecture is required where each mechanism has different resource requirements. Identification of the data type present in sensor network identifies the security threats to the communication for each data type. Every employing multitier security scheme is tailored to make the most out of the available resources. Use localized algorithm in which only one node heap all others sensors data and then sends this mix data to a sensor node which can communicate network and users [14].

The current protocols for data link layer and network layers are not adequate for handling various security threats in WSN. The proposed scheme in [15] is turn to account in the form of two layers, link and network layers. This strategy seep through the jumble attacks layer by layer to reduce the price of energy for processing. Type of attacks that proposed intrusion detection scheme in link layer can easily notice integrity, collision and exhausting attacks, and in network layer it behold sewage pool, wormhole, selective-forwarding and hello flood news attacks. This security architecture needed no extra component or hardware [15].

The Ad-hoc personal area network & Wireless Sensor Secure NETwork (AWISSENET) distributed detection system (DIDS) proposed in [16] for secure WSNs. The model has plug-in based design in order to enable a flexible management of the algorithms that running on each node. The local IDS agent is composed of four components. The plug-in manager, data manager, decision model and communication model. Intrusion algorithm runs just a subset of the AWISSENET nodes. The AWISSENET cluster can be multi-hop. The size of a cluster is nearly same scale as the number of bunches in network. The AWISSENET DIDS employs timestamps and absorbs, secrete keys are shared within each cluster and among the cluster heads. Timestamps are used to decide the freshness of the messages and stop replay attacks [16].

3.4 Schemes to Secure Ad-hoc Networks

The proposed system in [17] acts on control messages by checking the truthfulness of their content. Nodes operating the OLSR protocol keep neighborhood information's. All nodes of the network participate in IDS. This solution represents the first line of protection for the OLSR protocol. It alleviates threats exploiting flaws in the OLSR specifications to reroute the common routing operation [17].

A Grouped Black Hole Attack Security Model (GBHASM) mitigates the grouped malicious nodes to broadcast the shortest pathway through them to source and destination. Scheme is consisting of two modules; first module has the explanation about new node connectivity & communications. Server receives request acket from new node. It answers with membership acknowledgement to the node and stay for the acceptance. If node doesn't replay within a time limit, the server discards the joining request. Otherwise it throws its information. The information received by new joining node is placed in the database and also assign Node Code Pkk1 or pkk2.The second module handles all communication activities within the network. Once becoming a part of the network, the node drives call for shortest path through pkk2 packet. Each node will check pkk1 with pkk2, if key matches with in a given time limit, information will be released; otherwise the time of the packets to live, force it to become meaningless [18].

An effective wormhole attack defense method is proposed to limits the wormhole attacks on wireless ad-hoc network. In this method each new node of ad-hoc network collects information about one hope and two-hope neighbors, in this way the nodes construct a neighbor list and allocate a session key with all neighbor. The identity and MAC address is also present with a packet comes from every node. The next node then verifies whether the forwarder is a neighbor. This technique drops the replayed packet, and it broadcasts the exit of the wormhole [19].

A secure routing mechanism called security-aware ad-hoc routing (SAR) not only concern the length of the routers. The security metric is integral part of routing request or RREQ packet and change the forwarding behavior of the nodes receive on RREQ packet with a particular security matrix or trust level. SAR conforms that the node can only forward it, if the node itself can recommend the required security, otherwise the RREQ is discarded. If back-to-back path with the mandatory security elements can be found, an appropriate modified RREQ is launched from

an intermediate node or the ultimate destination. SAR can be employed, based on ad-hoc on-demand routing protocol such as AODV with suitable modification [20].

Domain		Challenges & Issues	Suggestions
Mobile Ad Hoc Networks		Cryptographic-based scheme may be failed to find out the intruders.	Use any proper intrusion detection system (IDS).
		Ad hoc network routing protocols are prone to security attacks.	Use any attack prevention scheme particularly at the time of root construction.
		Majority of routing protocols concern only the length of the routers.	The security metric should be integral part of routing protocols.
SENSOR NETWORK	Deployment Issues	WSN gateway form single point failure.	Fault endurance of WSN-gateway should be increase.
		After deployment sensor nodes are gone unattended.	Periodically checking all the attached nodes of a WSN.
	Protocol Issues	Current protocols for link layer and network layer can be failed to handle security threads in WSN.	Need for security architecture to handle this issue.
		No common model to guarantee security for each layer in WSN.	Holistic approach with respect to security can mitigate this issue.
	Inherited Issues	Limited computation power, short memory and low power supply.	Extensive research is required to resolve these inherited issues.
		Increment in the range of devices will increase the energy consumption.	
		Increment in the range will create high electromagnetic radiation.	
		Energy issue restricts the implementation of security schemes.	

Table 2. Major issues and Suggestions

4 CONCLUSION

In this survey paper, we look into the security issues and challenges in wireless communications, particularly in ad hoc communications. We have divided our studies into four sub-domains that are Security attacks, Vulnerabilities, Security models and Range limitation issues. Main issues addressed in this paper comprise the continuity of environment monitoring, limitation and vulnerabilities of sensors networks, the ad-hoc communication scheme, and the security scheme that protects against large number of attacks including DoS, Wormhole attacks, HELLO flood news attacks etc. we also discussed some security model for protection against attacks, these mechanisms still have limitations, which are discussed in this paper. We also provide a tabular form of major issues and challenges in WSN and MANETs and also provide some suggestion towards solutions. The contribution of this paper is to spell out the current security threats and other correlated issues in wireless communications and discussed

the proposed solutions which may offer a new way of thinking towards the solution space.

REFERENCES

[1] Kumar, R. Valdez, O.Gomez ,S.Bose: "Survivability evaluation of wireless sensor network under DDoS attacks"IEEE International Conference on Systems and Mobile Communications and Learning Technologies,2006 pp.82-82

[2] Tanveer A Zia and Md Zahidul Islam: "Communal Reputation and Individual Trust (CRIT) in Wireless Sensor Networks:"IEEE, International Conference on Availability, Reliability and Security, ARES '10 International Conference on, 2010 pp. 347-352

[3] H.R. Zeilandoo, M.A. Ngadi: "Intruder Location Tracking" second international conference on computer and electirical engineering, DO110.1109/ICCEE.2009.53, 2009 pp.507-511

[4] Xinyu Xing; Shakshuki, E.; Benoit, D.; Sheltami, T: "Security Analysis and Authentication Improvement for IEEE 802.11i Specification" IEEE lobal Telecommunications Conference, 2008. IEEE GLOBECOM 2008. pp. 1-5

[5] Boudriga, N.; Baghdadi, M.; Obaidat, M.S: "A New Scheme for Mobility, Sensing, and Security Management in Wireless Ad Hoc Sensor Networks"IEEE 39th Annual Simulation Symposium, November Digital Object Identifier: 10.1109/ANSS.2006.8, 2006.

[6] Todd Kennedy, Ray Hunt, Christchurch: "A Review of WPAN Security Attacks and Prevention" the International Conference on Mobile ..., 2008 - portal.acm.org

[7] Chi Yoon Jeong, Beom Hwan Chang and Jung Chan Na:, "A Survey on Visualization for Wireless Security" Networked Computing and Advanced Information Management, 2008. NCM '08. Fourth International Conference Volume: 1 , 2008.pp. 129-132

[8] Neel Diksha, Agarwal Shubham: "Backdoor Intrusion in Wireless Networks-Problems and Solutions" Communication Technology, 2006. ICCT '06. International Conference 2006 pp. 1-4

[9] Binod Vaidya, SangDuck Lee, Jongan Park: "Evaluation of Secure Multimedia Services over Wireless Access Network", Ubiquitous Multimedia Computing, 2008. UMC '08. International Symposium
, May 2008 pp. 181-184

[10] Hassen Redwan and Ki-Hyung Kim: "Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks" Frontier of Computer Science and Technology, 2008. FCST '08. Japan-China Joint Workshop , 2008 pp. 3-9

[11] Sarijari, M.A.B.; Rashid, R.A.; Rahim, M.R.A.; Mahalin, N.H: "Wireless Home Security and Automation System Utilizing ZigBee based Multi-hop Communication"Proceedings of IEEE 2008 6th National Conference on Telecommunication Technologies, August 2008 pp. 242-245.

[12] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong: "Security in Wireless Sensor Networks: Issues and Challenges" Advanced Communication Technology, 2006. ICACT 2006. The 8th International ConferenceVolume: 2 , Feb 2006 pp. 1048

[13] Ashraf, A.; Rauf, A.; Mussadiq, M.; Chowdhry, B.S.; Hashmani, M: "A Model for Classifying Threats and Framework Association in Wireless Sensor Networks" Anti-counterfeiting, Security, and Identification in Communication, 2009. ASID 2009. 3rd International Conference pp. 7-9

[14] Slijepcevic, S.; Potkonjak, M.; Tsiatsis, V.; Zimbeck, S.; Srivastava, M.B: "On Communication Security in Wireless Ad-Hoc Sensor Networks" Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002. Proceedings. Eleventh IEEE International Workshops,2002 PP.139-144

[15] Xi Peng; Zheng Wu; Debao Xiao; Yang Yu:"Study on Security Management Architecture for Sensor Network based on Intrusion Detection" Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC '09. International Conference on Networks Security, Wireless Communications & Trusted Computing,Vol. 2, 2009 pp. 503-507

[16] Lionel Besson, Philippe Leleu, Colombes Cedex France: "A Distributed Intrusion Detection System for Ad-Hoc Wireless Sensor Networks", Systems, Signals and Image Processing, IWSSIP 2009. 16th International Conference, 2009 pp.1-3

[17] Alia Fourati, Khaldoun Al Agha: "An IDS First Line of Defense for Ad-Hoc Networks", Wireless Communications and Networking Conference, 2007.WCNC 2007. IEEE pp. 2619-2624

[18] Shahid Shehzad Bajwa, M. Khalid Khan:"Grouped Black hole Attacks Security Model(GBHASM) for Wireless Ad-Hoc Networks" Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference Vol.1 , 2010 pp. 756-760

[19] Gunhee Lee, Dong-Kyoo Kim, Jungtack Seo: " An Approach to Mitigate Wormhole Attack in Wireless Ad-Hoc Networks"

Information Security and Assurance, 2008. ISA 2008. International Conference , 2008 pp. 220-225

[20] S Yi, P Naldurg, R Kravets - Urbana – Citeseer:" A Security-Aware Routing Protocol for Wireless Ad-Hoc Networks"