Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Review on the Network Security Related to Wireless Sensor Network

Akanksha Bali, Dr. Shailendra Narayan Singh
Computer Science and Engineering Department
ASET, Amity University, Noida,
Uttar Pradesh, India

Abstract— Network security is vital for securing all information that passed through network computer; hence network security is the most important element in information security. Security is one of the critical concern occurred in WSN due to limitations in computing and fixed resource. Wireless sensor network have a broad area of invaluable games, defence, civil, household, entertainment application. WSN nodes behave as information source by sensing and collecting sample of data from their environment. Energy efficiency, adaptive medium access control, scalability are the performance measures considered by WSN that posed interesting challenges to the community of engineers. The wireless sensor network is divided into four classes: threats to sensor network security, security requirements, attacks and security. The obstacles of sensor networks are fixed storage space and memory, drawback of power, unreliable and unattended operation. Security requirements are availability, self management, time synchronization, secure localization and authentication.

Keywords— WSN: wireless sensor network, Security of wireless network, Authentication, 4G wireless network, Application of WSN, Intrusion Detection, CWSN: cognitive wireless sensor network, Attacks, Wireless LAN, Internetworking, MANET.

I. INTRODUCTION

A sensor network consists of a large number of tiny, economical, self powered devices that can invigilate or sense, interact and compute with other devices for the motive of collecting local information to make universal resolution about a physical environment. WSN communicate with sensitive data and work in hostile area [21]. The WSN are vulnerable to various threats because they are physically reachable from the outside environment like interruption, interception, modification, fabrication and attacks like passive information gathering, node subversion, false node, node malfunction, node outage, message corruption, traffic analysis, selective forwarding, sink hole attacks and Sybil attacks. The confidentiality, integrity, authentication and availability are the four security goals towards sensor network [23]. WSN are promptly appearing as an important area in ubiquitous computing because eavesdropper can easily intercept the message and easily monitored the communication between the nodes; hence intrusion detection technique is important for ubiquitous applications that help in identifying the malicious intruder that is occupying the network domain [26]. Black hole attacks is same as DOS attack that occurs when the man in the middle change a set of nodes in the network to block the packets and produce incorrect/ changed messages instead of forwarding authentic information en-route the base station in WSN [38]. Authentication based intrusion prevention and energy saving intrusion detection are the two methods used to improve the defense of clustering based sensor network [19]. Intrusion detection techniques, cryptographic techniques, encryption and decryption, authentication by using id and password are used for providing security against WSN attacks. Cryptography is most vital for network security because cryptography is a developing technology and research on cryptography is required for authenticated communication [10]. The difference of wired and wireless network is that wireless network is more complex than wired network and because of its openness of transmission media, affected to security attacks that are inherited from wired networks. Wireless networks have higher channel error rate and limited resource than wired networks. The last one is that wireless network cannot used the security schemes defined by wired networks [42].

A. WLAN and INTERNETWORKING

The wireless technologies have different coverage and bandwidth drawback. So, no specific technology is considered as best. For ubiquitous wireless communication, internetworking among heterogeneous wireless network is most vital. 2G systems are not suitable for data communication. Limited capacity, eavesdropping, fraud are the problems in 1G that are successfully forwarded by 2G. These problems have been reduced in 3G systems as compared to 2G system. The integration of two security architectures named as 3G and WLAN produce an insecure outcome [12]. 3G and WLAN faces major security and performance challenges, exclusively for privacy and access control of mobile stations. When A.Duressi et al. try to access 3G services with the help of WLAN, they use hybrid 3G WLAN devices that help in location authentication of WLAN devices. They proposed threshold cryptographic tools to avoid security problem

created by scam among hybrid and WLAN devices [13]. The forthcoming wireless network that is 4G mainly focused on combining the wireless technologies by roaming among different wireless network that exist in the today worlds. The 4G wireless networks provide fast service and access for the mobile user [25].

B. MANETs

MANETs are the wireless networks need energy without any support of a static structure. In MANETs, mobile nodes can communicate with each other if they lie within radio ranges. They use multi-hop routing if the mobile nodes do not lie within radio range. The wireless link among the nodes in MANETs is highly vulnerable. Due to breakage of wireless link, topology of the mobile network is highly changing. No predefined boundary, attacker inside the network, no centralized control facility, finite energy resource is the security threats in MANETs. Availability, integrity, confidentiality, authenticity, authorization and anonymity are the security criteria in MANETs. DOS attacks, impersonation, routing attack and eavesdropping are some of the attacks occurred in MANETs. The Intrusion detection and cluster based ID are the security solutions used to deal with threats [16].

II. METHODOLOGY

A. *Security methods used in WSN:* - Several security techniques like cryptography, steganography and physical layer secure access are used to provide secure transmission of information.

1) *Cryptography:* - Encryption schemes needs extra bits, more processing extra battery and memory power. So, we don't apply encryption decryption techniques directly to the wireless sensor network which has tiny sensors and due to the lack of extra processing, memory and battery power. So, the main work of cryptography is to hide the contents of message to protect information.

2) *Steganography:* - Steganography differ from cryptography because it hides the occurrence of the message by embedding it into the image, video etc. The main goal of steganography is to modify official message so that it seems like ordinary message.

3) *Physical layer secure access:* -Frequency hoping is used by it in WSN. The main advantage of physical layer secure access is that hoping sequence is altered in less time. Due to well organized design that is needed to maintain a synchronized clock between the sender and the receiver.

B. *Security threats in WSN:* - The attacks occurred in wired networks are same as attacks in wireless networks. But some are aggravated due to the involvement of wireless sensor network. The unguided transmission medium is more prone to attacks than guided transmission medium that make WSN more vulnerable to security issues like attacks. Snooping problems occurs in WSN due to broadcast nature. The security mechanisms for wireless ad-hoc network cannot be applied directly to the WSN due to the variations in architecture of both networks. The centralized entity called sink is present in WSN which is absent in wireless ad-hoc network. WSN uses tiny sensor, but wireless ad-hoc network does not uses tiny sensors [9].

III. LITERATURE REVIEW

A.S.K Pathan et al. gives security scheme for wireless sensor networks. They provide the summary of various security schemes used in wireless sensor networks. JAM and warm hole based is one of the security schemes used to avoid DOS attack that is to avoid jammed region by using coalesced neighbor nodes and worm holes. They summarize statistical en-route filtering which is to prevent information spoofing which detects and remove wrong reports. They also summarizes security schemes like Radio resource testing, Random Key, Pre-distribution etc to prevent from Sybil attack, Bidirectional verification, multipath Multi-base station routing to prevent from hello flood attack on communication security, TIK, Random key distribution, Reward, Tiny-sec, snep and Utesla to protect from data spoofing, warm hole attack and information spoofing, data and information spoofing and attack in information in travel, data and information spoofing, black hole attacks, data or information spoofing and message replay attack, data and information spoofing and message replay attack respectively. A.S.K Pathan et al. proposed security in wireless sensor network under changing environment conditions by improving the performance of WSN with respect to connectivity, security, longevity. They proposed that holistic approach is better to apply than a single security solution for a single layer. If we follow the holistic view then overall network is secured by itself [9].

Araujo et al. works on security in cognitive wireless sensor network i.e. cognitive radio and analyzes how they could be used to reduce the negative effects. They show the complete taxonomy of WSNs with different attacks on purposes, targets and behavior.

A. *Communication Attacks:* - In this kind of attack, the attacker affects data transmission by isolating a node so that the behavior of the whole network is changed.

B. *Replay Attack:* - It consists of the repeat of message from inside or outside. Example message is focused to other than expected node. In CWSN, nodes shares information in terms of the whole network. Hence, it is overwhelmed more than WSN

C. *Jamming Attack:* - In Jamming Attack nodes used the radio frequencies that jams radio signal.

D. *Against Privacy Attacks:* - Attacker performs snooping through by taking same node information and easily finds the contents of communication.

E. *Traffic Analysis attacks:* - It extracts the information of content from nodes by analyzing snooping the traffic pattern on wireless communication. Example we can also find out that where the weakest spectrum zone is or where the primary users are emanating with the help of spectrum information.

F. *Impersonating Attacks:* - It acts like the original server node and joins to the network to receive packet and analyses the traffic, using CWS features.

G. *Node Targeted Attacks:* - It works by disrupting the nodes. It requires more attention than in a WSN because of the generation of information is important for the accurate working of CWSN. Example withdraws a cryptographic Key, changing the internal device code.

H. *Power Consumption Attacks:* - CWSN are more vulnerable to power consumption attacks due to small size of batteries and nodes. Example access point.

I. *Policy Attacks:* - Policy attacks are also classified into two types of attacks named as Excuse attack, Newbie Picking attack.

J. *Cryptographic Attacks:* - The main motive of cryptographic attack is to get the cryptographic key and analyze the weaknesses in system from transmission of information. Example Differential Power Analysis Attack (DPA).

K. *Sybil attack:-* In Sybil attack, a node can act to be more than one node means a node copy the identity of other real nodes in the Sybil attack. It harms the security of data, integrity because Sybil attacks attack the distributed storage, data aggregation and routing mechanisms. Efficient Protocols are used to prevent from this attack because wireless sensor networks have base stations or gateways.

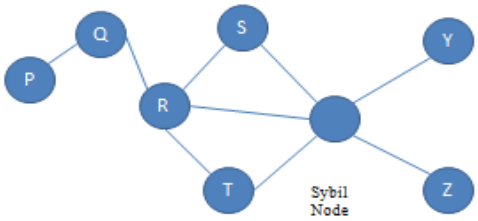

Fig 1: Sybil Attack [11]

L. *Black Hole Attack:* - This attack is also known as sink flow attack. In this attack malicious node alleged as the sink hole attack which has been able to insert between sink and sensor nodes and harms the packets passing between the communicating nodes.

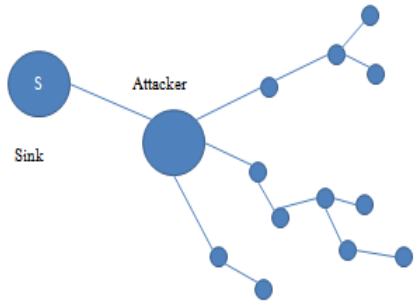

Fig2: Black Hole Attack [11].

M. *Warm Hole Attack:* - It occurs when the sensor initialize to discover the neighboring information and achieves the bit at one location and channel chose to another location of network.

Fig 3: Warm Hole Attack[11]

N. *DOS Attack:* - Dos attack disable the resources needed by the victim node by sending irrelevant packets and prevent real users from accessing services to which they are called. Dos attack is meant for attacker to disrupt a network as well as for any event that decline a service providing capability by networks.

TABLE 1: Dos attacks on Different layers [23]

Layers	**DOS Attacks**
Physical Layer	Jamming, Tampering
Link Layer	Collision, Disable Resources
Network Layer	Black holes, Misdirection
Transport Layer	Malicious Flooding, De-synchronization.

Author also found the remedies in CWSN which states that it suffer from a dangerous problem in security. They proposed various security schemes based on geo-location, Behaviour, reputation trust of the CR. If a primary user is initiated by the attacker, then the geo-location is an efficient method. They find that geo-location countermeasures do not appropriate for most of user cases. They conclude that some restrictions should be clearly defined while using the countermeasures depends on geo-location. Example restricted areas for fixed number of primary user or attacker in the scenario. Remedy based on behaviour tries to designing the distinction between a primary user and attackers. Genetic algorithms are used to find out the difference and recognize the identify behaviour and pattern changes, provide a good remedy for this problem. Versatility is the main advantage provided by the reputation system.

Araujo et all. faces many challenges and open problems in designing security schemes for cognitive WSNs. CWSN has many constraints , different features and less prone to eavesdropping because of lacking broadcast nature as compared to traditional WSNs. But cognitive features allow a changing reconfiguration to protect from attack. The Hostile environment is the second challenging factor studied by the author in which attacker can easily extract valuable information from the device and add incorrect information to the network. The third challenge faced by CWSN is the resource hungry security mechanism energy, communication and cognitive algorithms which are not cheap about money [11].

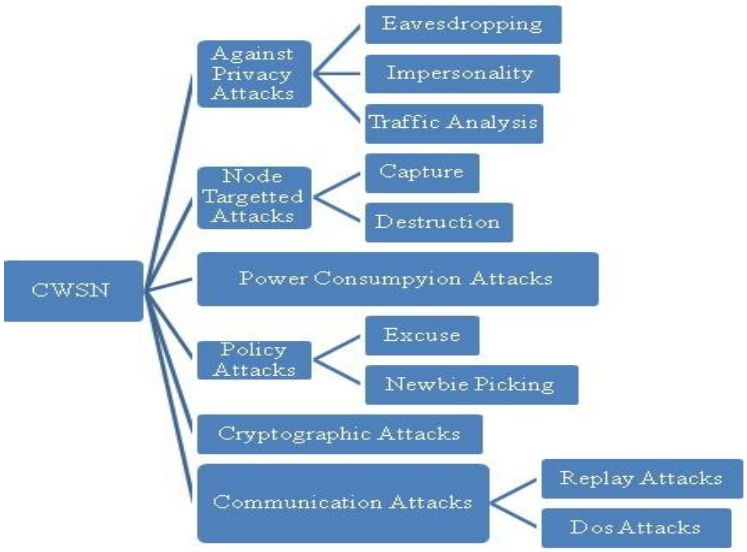

Fig 4: CWSN Attacks [11]

M.S.A.D Moura et al. propose secure multimedia mail system which is implemented by using java. It also discusses the network message delivery which is implemented by using RSA, MDS, DES and M/H message reception which is divided into three parts named as reception of the T-message, retrieval of its remote components and generation of the corresponding R-message. After all the process, M/H message visualization is done [17].

J. Yang et al. suggested authenticated key exchange protocol of the safe shared key. They use smart card and applying password base for providing trustworthy communications in the sensor network. They suggest the proposal key set protocol which did not use exponent arithmetic and the public key calculation prevents the man in the middle by applying ECDH to ach nodes associated with the key establishment process. The main operation used is XOR and hash calculations. The advantage of this protocol is that computational cost is less, secure in the guessing of password, secure from the server compromise attack [24].

D. He et al. proposed three classes of authentication scheme for the forthcoming 4G system. They introduced SPAKA which decreases the storage, communication load; computation of the user authentication depends on self certified public key [25]

B. Lee.et al. analyses security threat of WSN. They found that physical attack, attack of link level, attack to routing and transmission privacy, attack at application level, Node (BS) capture are threat to security. Simple network management protocol (SNMP), Sensor Network Management System (SNMS), Management Architecture for Wireless Sensor Network (MANNA) is all acts as the management of the entire network. They also introduced a security framework include system and security architecture which provide benefit to reliable sensor network management. This new scheme can also be applied to pervasive applications and effective in hierarchical sensor network [26].

Y. Wang et al. suggested a novel sine- curve mobility model by using single sensing and K- sensing analysing the effects of various intrusion paths on the probability of intrusion detection. This led to different conclusions. First one the lower bound for intrusion detection is provided by the immediate intrusion detection instead of employing mobility pattern. Second one is the flawless intrusion path that results in the least probability of intrusion detection by tuning the sine to line factor [28].

F.C jiang et al. states that the energy hole problem is one of the most security threat to WSN. They proposed a technique called queue based power saving technique that improve the lifetime security and provide a feasible solution that is cost efficient for the wireless sensor networks and mitigating the EHP. They use the ns2 simulator for evaluating the design [29].

A.S. Uluagac et al. give overview of TICK (Time Based Dynamic C keying and En-Route filtering) in which they explained various modules named as threat module, time based key management module, crypto module, filtering forwarding module. They compute the TICK window, evaluate the performance and compared with en-route filtering schemes. Tick removes malicious from the network have it is also called dynamic en-route filtering mechanism. They also found that TICK is feasible in the analytical and the simulation results. By comparing with other schemes, TICK was more energy efficient [30].

G. Vithya et al. gives overview of activation algorithm, adaptive routing protocol, video packet scheduling which proves that path which has minimum distance and has highest residual power are used when routing is done. They use poison model to search the route. They suggest the scheme which improves the transmission rate of video by utilizing scheduling algorithm for intelligent video packet [32].

V.P.V. gottumukkala et al. proposed techniques that use the blast nodes that surround the base station and route the packet using the shortest paths to select node. Blast node is a particular node which is chosen by the source that has a packet to send. The benefit is transmission delay and energy saving [35].

B.K Mishra et al. review various security algorithms to avoid black hole attack so that WSN make easy data delivery. They also found that false positive data still possible in the 100% successful data delivery [38].

H. Marzi et al. proposed new security model for wireless sensor network which offered greater accuracy in identifying trustworthy sensors which make security level of WSN stronger as compared to original sensors. EBTRM (Enhanced Bio Inspired Trust and Reputation system) uses more distance between client and trustworthy sensors as well as more energy consumption as compared with BTRM. They also found that there are constraints that occur due to energy, memory in terms of tiny device, unreliable communication, and higher latency in terms of multi hop routing [39].

B.B. Madaan et al. compares intrusion tolerance and fault tolerance. They uses SMP model for security quantification in which they show transition model of genetic state, behaviour of attacker and response of system. They also analysed the model like some markov model, SYN-flood dos attack model, MTTSF (Mean Time to Security Failure). They also detected probability distribution function that explain the behaviour of attacker and analyses the markov process for various security related attributes [41].

IV. APPLICATIONS

The applications are divided into On Body or Wearable Application and In Body or Implanted Application which is shown in the table below: [40]

TABLE 2: Applications of WSN

<table>
<tr><th colspan="2">On Body/Wearable Application</th><th>In Body/ Implanted Application</th></tr>
<tr><th>On Body Medical Application/ Wearable Medical Application</th><th>On Body Non Medical Application/Wearable Non Medical Application</th><th>In Body Medical Application/ Implanted Medical Application</th></tr>
<tr><td>Cannot be used inside, it is used at the close proximity of the user</td><td rowspan="2">Real Time Video streaming and Real Time audio streaming by using mp4 video player and mp3 respectively, body position and person location measurement Games and military Applications</td><td rowspan="2">Glucose sensor, endoscope capsule, Pacemaker, Sensor of Brain Liquid Pressure, cardiac records.</td></tr>
<tr><td>Temperature Estimation, Respiration and Heart Rate invigilator, PH and glucose sensor, Pulse oximeter</td></tr>
</table>

V. CONCLUSIONS

In this paper, we have reviewed a number of problems related to security in CWSN. We have reviewed Security requirements, Attacks, threats, security methods, 4G wireless networks, Black hole Security and various futuristic applications. Deployment of sensor networks in the absence of security is harmful to variety of attacks. On the basis of our conclusion, we persuade the need of demand a security framework like intrusion detection techniques, cryptographic techniques like encryption and decryption techniques to provide remedy against attacks in WSN. The integration of two security architectures named as 3G and WLAN produce an insecure outcome. Security is a mandatory factor for CWSN.

REFERENCES

[1] H Yang, H. Luo, F. Ye, S. Lu, L. Zhang, "*Security in Mobile Adhoc Networks: Challenges and Solutions* ", 1536-1284 © 2004 IEEE, pp. 38-47.

[2] M. A. Ameen, J. Liu, K. Kwak, "*Security and Privacy Issues in Wireless Sensor Networks for Healthcare Applications*", Springer, 2012, pp. 94-101.

[3] S.K Singh, M.P Singh, D. K. Singh, "*A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks*", ISSN: 2231-2803 IJCTT, pp. 1-9.

[4] U. Varshney, "*Wireless I: Mobile and Wireless Information Systems: Applications, Networks, and RESEARCH Problems* ", Department of Computer Information Systems, Georgia State University, Atlanta, Georgia, U.S.A, Vol. 12, 2003, pp. 155-166.

[5] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A.W. Jackson, "*Survivable Mobile Wireless Networks: Issues, Challenges, and Research Directions*", ACM, Atlanta, Georgia, U.S.A, 2002, pp. 31-40.

[6] C. Karlof, N. Sastry, D. Wagner, "*TinySec: A Link Layer Security Architecture for Wireless Sensor Networks*", ACM 1-58113-879-2/04/0011, 2004, pp. 162-175.

[7] Y. Zhang, W. Lee, "*Intrusion Detection in Wireless Ad-Hoc Networks* ", ACM 1-58113-197-6/00/08, 2000, pp. 275-283.

[8] T. Kavitha , D. Sridharan, "*Security Vulnerabilities in Wireless Sensor Networks: A Survey*", Journal of Information Assurance and Security, 2010, pp. 031-042.

[9] A. S. K. Pathan, H. W. Lee, C. S. Hong, "*Security in Wireless Sensor Networks: Issues and Challenges*", ISBN 89-5519-129-4 ICACT, 2006, pp. 1043-1048.

[10] S. Kaushik, A. Singhal, "*Network Security Using Cryptographic Techniques*", ISSN: 2277 128X IJARCSSE, Vol 2, Issue 12, 2012, pp. 105-107.

[11] A. Araujo , J. Blesa, E. Romero and D. Villanueva, "*Security in cognitive wireless sensor networks. Challenges and open problems*", Journal on Wireless Communications and Networking, Springer, 2012, pp. 1-8.

[12] M. SHIN, J. MA, A. MISHRA, AND W. A. ARBAUGH," *Wireless Network Security and Interworking*",0018-9219 © 2006 IEEE, Vol. 94, No. 2, pp. 455-466.

[13] A. Durresi and M. Durresi, "*Secure Spatial Authentication for Mobile Stations in Hybrid 3G-WLAN Serving Network*", 0-7695-3102-4/08 © 2008 IEEE The Third International Conference on Availability, Reliability and Security, pp. 1325-1339.

[14] D. K. Mishra, "*Privacy Preservation in MANET: Issues and Challenges* ", 978-0-7695-4668-1/12 © 2012 IEEE 2012 Third International Conference on Intelligent Systems Modelling and Simulation, pp. 13.

[15] M. He, L. Chen, H. Wang, Z. Gong, Z. Liu, " *Survey on Secure Transmission of Network Coding in Wireless Networks*", 978-0-7695-4719-0/12 © 2012 IEEE International Conference on Computer Science and Service System, pp. 1216-1219.

[16] R. Sheikh, M. S. Chandel, D. K. Mishra, "*Security Issues in MANET: A Review* ", 978-1-4244-7202-4/10©2010 IEEE.

[17] M.S.A.D. Moura, G.L.D.S. Filbo, T.V. Batista, L.F.G Soares, "*SMMM-A Secure Multimedia Mail System*", 0-7803-6536-4/00 2000 IEEE, pp. 1501-1504.

[18] R.Rao, G. Kesidis, " *Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth* ", 0-7803-7974-8/03 © 2003 IEEE, pp. 2957-2961.

[19] C.C. Su, K.M. Chang, Y.H. Kuo, M.F. Horng, " *The New Intrusion Prevention and Detection Approaches for Clustering-based Sensor Networks*", 0-7803-8966-2/05 © 2005 IEEE Communication Society, pp. 1927-1932.

[20] L.P. Gaspary, R.N. Sanchez, D.W. Antunes, E. Meneghetti, "*A SNMP-Based Platform for Distributed Stateful Intrusion Detection in Enterprise Networks*", 0733-8716 © 2005 IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 23, NO. 10, pp. 1973-1982.

[21] M.I.A.E. BArr, M.M.A. Otaibi, M.A Youssef, " *Wireless Sensor Networks- Part II: Routing Protocols and Security Issues* ", 0-7803-8886-0/05 ©2005 IEEE CCECE/CCGEI, Saskatoon, pp. 69-72.

[22] N. Boudriga, M.S. Obaidat, "*Mobility and Security Issues in Wireless Ad-hoc Sensor Networks*",0-7803-9415-1/05 ©2005 Globecom, pp. 2777-2781.

[23] T. Zia, A. Zomaya, "*Security Issues in Wireless Sensor Networks* ", 0-7695-2699-3/06 (c) IEEE.

[24] J. Yang, C. Seo, J. Cho, " *A Three – Party Authenticated Key Exchange Cryptosystem for Secure Key Exchange in Wireless Scheme Smartcard using Elliptic Curve Sensor Network*" 1-4244-0216-6/06 ©2007 IEEE.

[25] D. He, J. Wang, Y. Zheng, "*User Authentication Scheme Based on Self-Certified Public-Key for Next Generation Wireless Network*" , 1-4244-2427-6/08 ©2008 IEEE.

[26] B. Lee, S. Bae, D Han, "*Design of Network Management Platform and Security Framework for WSN*", 978-0-7695-3493-0/08 IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008, pp. 640-645.

[27] J.S. Li, C.F. Yang, "*Quantum Communication in Distributed Wireless Sensor Networks*", 978-1-4244-5113-5/09 2009 IEEE, pp. 1024-1029.

[28] Y. Wang, Y.K. Leow, J. Yin, "*Is Straight-line Path Always the Best for Intrusion Detection in Wireless Sensor Networks*" 1521-9097/09 © 2009 IEEE 15th International Conference on Parallel and Distributed Systems, pp. 564-571.

[29] F.C. Jiang, H.W. Wu, D.C. Huang, *"Lifetime Security Improvement in Wireless Sensor Network using Queue-based Techniques*", 978-0-7695-4236-2/10 © 2010 IEEE International Conference on Broadband, Wireless Computing, Communication and Applications, pp. 469-474.

[30] A.S. Uluagac, R.A. Beyah, J.A. Copeland, "*Time-Based Dynamic Keying and En-Route Filtering (TICK) for Wireless Sensor Networks*", 978-1-4244-5638-3/10 ©2010 IEEE.

[31] V. Casola, A.D. Benedictis, A. Mazzeo, N. Mazzocca, "*SeNsIM-SEC: security in heterogeneous sensor networks*", 978-1-4577-0737-7/11 ©2011 IEEE.

[32] G.Vithya, B.Vinayagasundaramz, "*Actuation Sensor with Adaptive Routing and QOS Aware Checkpoint Arrangement on Wireless Multimedia Sensor Network*", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011, pp. 444-449.

[33] H. Modares, R. Salleh, A. Moravejosharieh, "*Overview of Security Issues in Wireless Sensor Networks*", 978-0-7695-4562-2/11 © 2011 IEEE Third International Conference on Computational Intelligence, Modelling & Simulation, pp. 308-311.

[34] V. C. Sekhar, M. Sarvabhatla,"*Security in Wireless Sensor Networks With Public Key Techniques*", 978-1-4577-1583-9/ 12 © 2012 IEEE: International Conference on Computer Communication and Informatics.

[35] V.P.V. Gottumukkala, V. Pandit, H. Li and D. P. Agrawal, "*Base-station Location Anonymity and Security Technique (BLAST) for Wireless Sensor Networks*", 978-1-4577-2053-6/12 ©2012 IEEE International Workshop on Security and Forensics in Communication Systems, pp. 6705-6709.

[36] D. Shan, K. Zeng, W. Xiang, P. Richardson, Y. Dong, "*PHY-CRAM: Physical Layer Challenge-Response Authentication Mechanism for Wireless Networks*" 0733-8716/13 c 2013 IEEE Journal on Selected Areas in Communications, Vol. 31, NO. 9, pp. 1817-1827.

[37] J. Suryadevara, B. Sunil, N. Kumar, "*Secured Multimedia Authentication System for Wireless Sensor Network Data related to Internet of Things*" 978-1-4673-5221-5/13©2013 IEEE Seventh International Conference on Sensing Technology, pp. 109-115.

[38] B.K. Mishra, M.C. Nikam, P. Lakkadwala, "*Security Against Black Hole Attack In Wireless Sensor Network–A Review*" 978-1-4799-3070-8/14 © 2014 IEEE Fourth International Conference on Communication Systems and Network Technologies, pp. 615-620.

[39] H. Marzi, A. Marzi, "*A Security Model for Wireless Sensor Networks*" 978-1-4799-2614-5/14 © 2014 IEEE, pp. 1-6.

[40] S. Ullah, P. Khan, N. Ullah, S. Saleem, H. Higgins, and K. Sup Kwak, "A Review of Wireless Body Area Networks for Medical Applications", arXiv:1001.0831v3 [cs.NI] 3 Aug 2010, pp. 1-7.

[41] B. B. Madan, K.G. Popstojanova, K. Vaidyanathan, K. S. Trivedi, "*A Method for Modelling and Quantifying the Security Attributes of Intrusion Tolerant Systems*", ELSEVIER, 2004, pp. 167-186.

[42] J. Zhu and J. Ma, "*A New Authentication Scheme with Anonymity for Wireless Environments* ", 0098 3063/04 © 2004 IEEE, pp. 231-235.

