2016 1st International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia

Adaptive Security for Multilevel Adhoc Networks – A Survey

Tahira Mahboob, Samman Fatima, Zunaira Atta
Department of Software Engineering
Fatima Jinnah Women University
The Mall, Rawalpindi, Pakistan
tahira.mahboob@yahoo.com

Abstract **- An adhoc network does not depend on any fixed structure or mechanism, unlike other types of networks. These have been widely in use for commercial purposes due to their unique properties. With major advantages of diversity offered by adhoc networks security is one of the greatest challenges faced by adhoc networks. The present study has been mainly dedicated towards highlighting various threats and challenges faced by ad-hoc networks. The scope of the study has been set for academia and research. This study aims to serve as an aid towards developing and understanding of adoption of required security for multi-level adhoc networks. Diverse security mechanisms, protocols, security threats/attacks, challenges and algorithms for securing ad-hoc networks are discussed in detail.**

Keywords*—dynamic decentralized hybrid MAC(DHMAC),* Location Based Geocasting and Forwarding(LGF), *mobile adhoc network (MANET), On-Demand Distance-Vector(AODV)*

I. INTRODUCTION

An ad-hoc network is mobile network which is connected through scattered wireless nodes without need of central infrastructure. In this system each individual node is free/mobile and is able join the network without any fixed infrastructure of communication and can share resources with each other. [1] Because of distributed nature it is subjected to varied malicious attacks and hence difficult to propose a comprehensive security model for the multilevel adhoc networks. Several models have been proposed that provide security/confidentiality to the data communications. Secure routing algorithms are main focus of some researchers. While others focuses on a proper security framework for distributed routing and access mechanisms.

The sections of the research paper are Literature Review in Section II, Security of Multilevel-Adhoc networks in Section III, Threats/Challenges to Adhoc Networks in Section-IV followed by Conclusion in Section-V.

II. LITERATURE REVIEW

In 2005, Scott, Donald[2] discussed the difficulties in time management in (ad-hoc networks), he also introduced the Ariadne protocol that uses Timed Efficient Streaming Loss-tolerant Authentication (TESLA) protocol, TESLA uses one way hash function to overcome limitations in nodes by using less synchronization between nodes. For applying this protocol a clock has been used to synchronize. One of the possible disadvantages to the protocol is synchronization delay which can be minimized through using better clock synchronization.

Security risks concerned with adhoc networks were discussed by Donadio, Antonio, and Giorgio [3].The process and the suitable framework that is being taken into account for reducing the risks of security is analyzed. A grid based system for the detection of attacks and security threats is proposed that serves as traffic analyzer. It observes and calculates the traffic load, the feedback and results and provide all the information to neighboring nodes.

In the same year, Cha, Hyun-Jong, In-Sung Han, and Hwang-Bin Ryou[5] evaluated the route availability time of availability of route from one node to another using Ad hoc On-demand Distance Vector(AOMDV). An AOMDV choose the node on dynamic basis.

Shah, Munam Ali, Sijing Zhang, and Carsten Maple [5] discussed the cognitive wireless points that sense vacant channels in the environment, after exchanging control information, agreeing on free channel list for transmission of Information. ”A dynamic decentralized and hybrid MAC” is presented (DHMAC) in the study. It searches the vacant spaces and sets one vacant space as “Primary Control Channel” (PCCH) for exchanging control information. This gives extra security to the system. This protocol also helps to analyze jamming attacks.

Various techniques for detecting black hole attacks, denial of service attack were discussed by Jain, Sakshi, and Ajay [6]. Author identifies that a false node claims to be shortest routing path and then absorb all packets without sending. Five prevention techniques are presented in paper. First one uses destination sequence number, asymmetric technique, opinion from other nodes, trust among nodes and using extra nodes for detection. All these techniques help in detecting as well as removing black hole attacks subjected to network.

A solution towards heterogeneous attacks in ad-hoc networks was proposed recently in 2015 by Babu, E. Suresh, C. Nagaraju, and M. H. M. [7]. Inspired Biotic Hybrid Cryptographic mechanism using less bandwidth and memory as compared to other systems was proposed. It provides better security mechanism and less effort.

Mohamed [8] presented immune based security architecture for the simulation of number of HIS processes for securing the

MANET along with negative selection theory and danger theory for a strength, robustness and scalability of system. A CPN model for detection of problems and security threats to the network and propose a model for protection.

Sathish P. Alampalayam and Anup Kumar [9] presented an adaptive security system to tackle the DOS attacks (denial of service) automatically in ad-hoc networks based mobiles. Proposed system is implemented by feedback based approach which helps to maintain the security level.

Yang, Hao, HaiyunLuo, Fan Ye, Songwu Lu, and Lixia Zhang [10]. Presented the fundamental problems in the multi-level networks connectivity in MANET (mobile ad hoc networks) along with the solutions. They proposed (one or two way) HMAC key chain authentication codes for the secure routing between all the nodes of network.

Xie, Bin, and Anup Kumarhave[11] presented effective solutions for the security problems in non-adversarial integrated networks. They presented a mechanism in which "modified minimal public" protocol was used, for discovery of correct route and control of access network; malicious nodes are also presented from getting into network by it.

Chigan, Chunxiao, Leiyuan Li, and Yinghua Ye [12] presented the framework to solve the problems regarding resource aware self-adaptive security in MANET. They proposed techniques to maximize overall performance, capability and security of network without any security attack.

Chen, Tieming, Jie Jiang, Bo Chen [13], and JiameiCai presented threshold signatures approach. Management system based on certificates was proposed for the security of networks, which is scalable and dynamic for ad hoc networks. They also presented detailed algorithm and threshold model of the proposed techniques.

Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M.[14] discuss the security of adhoc networks using routing mechanism security techniques. AODV and DSR protocols have been analyzed for providing security. The proposed algorithm (ARAN) is based on certificates and successfully beats the attacks using various scenarios.

Authors [15] propose a scheme implemented in a fully distributed manner in order to protect against attacks without the need to depend on faculty hardware. Several optimization techniques have been proposed targeting improved efficiency of Delay tolerant networks (DTNs). The models have been implemented using simulation techniques.

The location-based geocasting/forwarding routing protocol (LGF) discussed by Latiff, L. A., Ali, A., Ooi, C. C., & Fisal, N [16] is based on location information. It has several advantaged and the main highlighted one is the reduction in overhead over flooding and routing. Only the nodes that are present in forwarding zone participate in rebroadcasting and flooding is reduced. The implementation of the LGF in a real MANET test bed is outline in this study/paper using GPS-free indoor location tracking mechanism with geocast-enhanced AODV.

Konate, K., & Gaye, A. [17] in 2011 dedicated their research to study attacks and contremusure in MANET. Author discusses attacks such as cooperative Black hole, Blackmail, Overflow, Selfish and analyze these attached in detail with the help of simulation tool ns2.

III. SECURITY OF MULTILEVEL ADHOC NETWORKS

Security is very important aspect while communicating our information or data. Sometimes secure communication becomes crucial because the information that is being communicated is very important and we must have to protect it from our enemies or hackers, for the sake of our survival and welfare or, i.e. information regarding military must be protected from all types of threats. It has become somehow difficult in military environments because infrastructures of our networks has proven vulnerable to security threats and various attacks and could break down the security of servers. In order to resolve these issues and to protect our systems from such attack; a security structure is evaluated for multilevel and ad hoc networks with Unmanned Aerial Vehicles (also known as drone or aircraft that is controlled by a remote) usually used in battlefields.

The structure is used to adapt the similar or dependent damages on the network. The infrastructure used to control the security has two modes. First is infrastructure and second is infrastructure less mode. Different protocols are anticipated for multilevel and ad hoc networks. These protocols are commonly used for making ad hoc networks to homogeneous networks. In homogeneous networks all connection in the network has equal authority for transmission of data and has same access to the channel with same frequency.

The protocols that are being used for routing are affected by the size of network. And hence affect the throughput of network. Each connection has to share it bandwidth with connection near to it, this is the main reason for the slow routing in homogeneous channels. Issues in the multilevel ad-hoc networks had overcome by proposing UAVs along with heterogeneous and ad-hoc networks.

The following contents of the paper discuss security of multilevel network with the example of UAV-Backbone Nodes followed by the Adaptive Security Model for adhoc Networks. Different security attacks are also explained in later sections and then challenges to proposed system are mentioned.

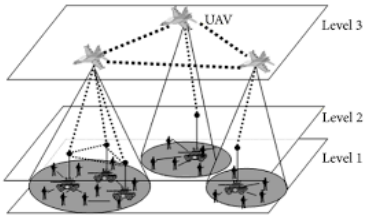

Fig.1. Mobile Adhoc Network Architecture

In this paper security is concerned in a network so it means the secure communication between the nodes or connections. The infrastructures of our multilevel ad-hoc networks and private area networks have proven vulnerable to security threats and various attacks. There are number of attacks i.e. MANET attacks (active attack, passive attacks), wormhole, black hole and network layer attacks. Traditional techniques used to maintain the security are not adequate for the future use or latest ad hoc networks such as PAN (private area network) and MANET. For protecting our network systems from these risks multiple security structures or models are evaluated for multilevel and ad hoc networks. Such as adoptive security model, UAVs network technology for multilevel networks. It is mostly used for battle purposes or undercover purposes such as spying.

A. Unmanned Aerial Vehicles-Mobile Backbone Nodes Networks (UAV-MBNs):

The heterogeneous ad hoc and multilevel networks are also named as UAVs and UAV-MBN [18].As discussed above, these networks works in two types of modes which toggle according to the situation and need of structure and has three layers. (The infrastructure and less infrastructure mode) Both are implemented on the drones or remote control aircrafts depending upon the situation. In first mode the security and authentication services are applied on the drone which decreases the problems by enhancing the flexibility so it becomes manageable. Incase drone is damaged or destroyed; the system manages to toggle to the other mode which is less infrastructure mode.

- Ground connections or nodes compose first layer, which consist of soldiers having limited devices for communicate or computation. They communicate through broadcast wireless channels of limited range.
- The second layer consists of special units for fight such as trucks and tanks having more capabilities for communication and computation than the first layer. They also have point to point communication links of higher bandwidth for effective communication. These layers collectively act as ad hoc network wireless network and the mode on the layers is fewer infrastructures as long as third layer is absent.
- The third layer is composed by UAV-MBN which has drone that flies over the height or 50 feet having phased array antenna in order to keep its connection with LOS (line of sight) with area where operation is being held. All VAVs formed Mobile backbone and are inter-related to each other. They operate in infrastructure mode and have very quick access to the medium.

B. Adaptive Security Model:

This security model is used for the security of various parameters with in a network and monitors all the nodes. If there is a threat of a security attack ASM model corrects the changes after taking spontaneous actions. [19]. Where SL is the normal security level that represents the starting level for holistic security related to routing attacks and VL represents the vulnerability level evaluated by the vulnerability evaluation framework from the measured metrics. The basic frame work is shown in the figure.

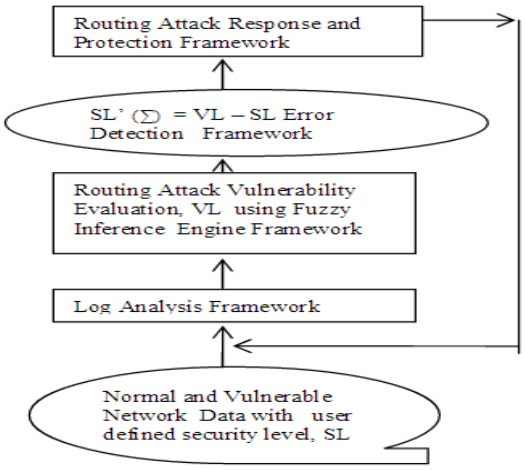

Fig.2 Architecture of ASM

Note: SL: security-level (starting level for holistic security) and VL: vulnerability level (vulnerability evaluation framework from the measured metrics).

Algorithm for ASM:

Algorithm of the proposed model shown in the Figure 1 can be indicated in the following steps:
Step 0: Input SL as specified by the security policy of the user for a given system. For the first iteration SL' is assumed to be SL. Execute Step2.
Step 1: Compute SL'= VL – SL; If SL' > 0, reduce the security level by that number and if SL' < 0, increase the security level by that number.
Step 2: SL' is applied to the protection framework which triggers the appropriate security policy in the protection framework module based on the value of SL'.
Step 3: System reacts with the given security features and possible attacks.
Step 4: Measure the characteristics (metrics) of the distributed system.
Step 5: Input the measured variables to fuzzy inference system.
Step 6: Get the VL as the output from the fuzzy inference vulnerability evaluation module.
Repeat Step 1 to Step 6 as long as the system returns to normal SL level.
Alternatively Step 1 can be replaced by a trained ANN which takes in SL and VL of previous iterations as inputs and sets the SL' to adapt to normal security level.

C. *Secure Communications in Adhoc Networks(Protocols and Models):*

There are many other protocols used for secure communication among all nodes of a network. LGF Protocol (Location Based Geocasting and Forwarding) Prevents wormhole (fake tunnel to access the data between two actual nodes) by verifying the IP for each node. [16] AODV Protocol (Adaptive On-Demand Distance-Vector) for the prevention of black hole i.e. attacks in which a node acts maliciously and is added to the network and hence the packets are lost.) By providing the security during the discovering of route mechanism and data transfer mechanism [4] [14].

Several other protocols have been proposed for secure communication on the adhoc network due to inherent lack of security provision and unavailability of defense against malicious attacks such as the de-facto MAC(medium access control IEEE 802.11 protocol)[20] Protocol, traditional AODV(on demand distance vector protocol)[21] and the DSR(dynamic source routing protocol). Secure distance vector protocol was proposed by Hu, Y. C., Johnson, D. B., & Perrig, A. [22] [23].

Authors have proposed several models for secure communication such as the RIOMO protocol by Rahman, S. M. M., Inomata, A., Okamoto, T., Mambo, M., & Okamoto, E. in 2007[24] or the protocol suite design by Panagiotis Papadimitratos using concept of certificates [25] [26]. In 2014 the security concern of authentication in adhoc network was discussed by Manoj, S. M., & Vasundra, S [27] in their research 2014.

IV. ATTACKS AND CHALLENGES TO SECURITY AD-HOC NETWORKS

A. *Threats to Adhoc Networks:*

a) Rushing Attack: The rushing attack prevents previously published on demand routing protocol to find routes longer than 2 nodes [28].

b) Barrage and Sleep deprivation Attack: Proposed by San Jao [29] [30]. The target is a sensor node in the adhoc network whose one primary purpose is to conserve power where this attack deprives it from doing so by interacting in a legitimate manner. It prevents victim to go to sleep model [31]. In barrage attack the victim is bombarded with request messages to waste power resources unlike sleep deprivation attack that send requests only as much as necessary to keep it alive/responding.

c) Gray Hole attack: A gray-hole attack, attacks to Ad Hoc AODV protocol and shows itself as a desired route, moreover a gray-hole attack may also drop some of the packets going to coming from destination or source. Some types of gray-hole attacks works maliciously for some time and after that time they become normal. [32]

d) Sinkhole attacks: In sinkhole attack, a node shows tries to catch the neighboring packets and gets access to data of these nodes. The trust of a packet coming from some source is measured through probabilistic protocol that helps to minimize sinkhole attack [33].

e) Misdirection attacks: In Misdirection attacks, a false node tries to misdirect packets to it or towards some other nodes [34].

f) Worm Hole Attack: in this attack, the packets are recorded by malicious node, from one location and are saved to another location. This false routing disturbs the network. It can make true by using encryption algorithm and location information [35].

g) Black Hole Attack: This attack claims absorbs packets without forwarding them by claiming false routing. In this approach the receiver node after receiving a packet confirms through destination whether it has sent the packet or not, the false node is detected when no route to destination is available [36].

h) Selfish Attack: Discussed by [37]; a selfish attack occurs when a node acting as forwarding service provider will forward packets received from nodes with stronger link when resources are limited.

B. *Challenges to Ad-hoc networks*:

Both challenges and incentives are there in Ad-hoc networks. These could be subjected to various attacks which can misdirect the packets, absorb packets, delete packets, and modify packets view data of packets and packets distortion which cause confidentiality issues. Also, a node having poor physical protection has a high possibility of being compromised. A node within a network may also acts maliciously, therefore, the attacks from within a network shall also consider. To maximize security, an ad-hoc network should not consist of any centralized node, so that whole network is not compromised if a central entity is being compromised. The security mechanism of multilevel ad-hoc network should be efficient enough so that it can handle multiple nodes in the network.

One the most apparent challenges faced by adhoc network is the inherent broadcast medium (wireless) which is susceptible to eavesdropping. The other issue is the lack of infrastructure and instability in network formation as nodes are mobile, physical placement of nodes again is a concern specifically when used for military purposes/sensitive

environments, scalability is again an eminent challenge in adhoc networks. Yet again the issue of secure routing/communication mechanism is an ever evolving issue for network users/administrators [38] [39].

Various solutions have been proposed to attain secure communication and authentication within the adhoc network as discussed in the text earlier. Nevertheless, as the secure mechanisms tend to evolve over time the malicious attacks and threats also emerge consequently. The race seem to continue as one cannot deny the effectiveness of adhoc networks for efficient/cost effective network architecture solution [40].

V. CONCLUSION

In multilevel ad-hoc network, secure routing is biggest challenge. Secure routing can achieved through different techniques, algorithm and protocols as ASM, AODV and LGF. This paper discusses the various mechanisms for secure routing. The ad-hoc networks are challenged by various attacks as well, which are also addressed in this paper such as Worm Hole, Sinkhole, Black Hole, Gray hole, Barrage and Sleep deprivation attack, Selfish attack, and Misdirection attacks. These attacks can compromise a whole network. One can remember these attacks while designing a security mechanism for ad-hoc networks. So to protect our system from such attacks we used some techniques UAVs multilevel and ad hoc network, ASM model, RIOMO protocol, AODV protocol and LGF protocols. The ever evolving nature of wireless networks specifically adhoc networks makes it inherently more and more significant to provide a secure mechanism for communication and routing of information for the users/administrators of such networks.

REFERENCES

[1]. Perkins, C. E. (2001). Ad hoc networking (Vol. 1). Reading: Addison-wesley.

[2]. Scott, Donald J. "Relying on time synchronization for security in ad hoc networks." In Proceedings of the 43rd annual Southeast regional conference-Volume 2, pp. 87-91. ACM, 2005.

[3]. Donadio, Pasquale, Antonio Cimmino, and Giorgio Venture. "Enhanced intrusion detection systems in ad hoc networks using a grid based agnostic middleware." In Proceedings of the 2nd international workshop on Agent-oriented software engineering challenges for ubiquitous and pervasive computing, pp. 15-20. ACM, 2008.

[4]. Cha, Hyun-Jong, In-Sung Han, and Hwang-Bin Ryou. "QoS routing mechanism using mobility prediction of node in ad-hoc network." In Proceedings of the 6th ACM international symposium on Mobility management and wireless access, pp. 53-60. ACM, 2008.

[5]. Shah, Munam Ali, Sijing Zhang, and Carsten Maple. "A Novel Multi-Fold Security Framework For Cognitive Radio Wireless AdHoc Networks." In Automation and Computing (ICAC), 2012 18th International Conference on,pp. 1-6. IEEE, 2012.

[6]. Jain, Sakshi, and Ajay Khunteta. "Detection Techniques of Blackhole Attack in Mobile Adhoc Network: A Survey." In Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015), p. 47. ACM, 2015.

[7]. Babu, E. Suresh, C. Nagaraju, and M. H. M. Prasad. "A Secure Routing Protocol against Heterogeneous Attacks in Wireless Ad-hoc Networks." InProceedings of the Sixth International Conference on Computer and Communication Technology 2015, pp. 339-344. ACM, 2015.

[8]. Mohamed, YasirAbdelgadir, and Azween B.Abdullah. "Immune inspired framework for adhoc network security." In Control and Automation, 2009. ICCA 2009. IEEE International Conference on, pp. 297-302. IEEE,2009.

[9]. Alampalayam, Sathish P., and Anup Kumar. "An adaptive security model for mobile agents in wireless networks." In Global Telecommunications Conference, 2003. GLOBECOM'03. IEEE, vol. 3, pp. 1516-1521. IEEE, 2003.

[10]. Yang, Hao, HaiyunLuo, Fan Ye, Songwu Lu, and Lixia Zhang. Security in mobile ad hoc networks: challenges andsolutions." Wireless Communications, IEEE 11, no. 1 (2004): 38-47.

[11]. Xie, Bin, and Anup Kumar. "A framework for integrated Internet and ad hoc network security." In Computers and Communications, 2004.Proceedings. ISCC 2004. Ninth International Symposium on, vol. 1, pp. 318-324. IEEE, 2004.

[12]. Chigan, Chunxiao, Leiyuan Li, and Yinghua Ye. "Resource-aware self-adaptive security provisioning in mobile ad hoc networks." In Wireless Communications and Networking Conference, 2005 IEEE, vol. 4, pp. 2118-2124. IEEE, 2005.

[13]. Chen, Tieming, Jie Jiang, Bo Chen, and JiameiCai. "A dynamic and Scalable security framework for ad-hoc sensor network." In Wireless, Mobile and Multimedia Networks, 2006 IET International Conference, pp. 1-4.IET, 2006.

[14]. Sanzgiri, K., Dahill, B., Levine, B. N., Shields, C., & Belding-Royer, E. M. (2002, November). A secure routing protocol for ad hoc networks. In Network Protocols, 2002. Proceedings. 10th IEEE International Conference on (pp. 78-87). IEEE.

[15]. Zhu, H., Lin, X., Lu, R., Fan, Y., & Shen, X. (2009). Smart: A secure multilayer credit-based incentive scheme for delay-tolerant networks. IEEE Transactions on Vehicular Technology, 58(8), 4628-4639.

[16]. Latiff, L. A., Ali, A., Ooi, C. C., & Fisal, N. (2005, July). Location-based geocasting and forwarding (LGF) routing protocol in mobile ad hoc network. In Advanced Industrial Conference on Telecommunications/Service Assurance with Partial and Intermittent Resources Conference/E-Learning on Telecommunications Workshop (AICT/SAPIR/ELETE'05) (pp. 536-541). IEEE.

[17]. Konate, K., & Gaye, A. (2011, January). Attacks Analysis in mobile ad hoc networks: Modeling and Simulation. In 2011 Second International Conference on Intelligent Systems, Modelling and Simulation (pp. 367-372). IEEE.

[18]. Alampalayam, S. P., & Kumar, A. (2003, December). An adaptive security model for mobile agents in wireless networks. In Global Telecommunications Conference, 2003. GLOBECOM'03. IEEE (Vol. 3, pp. 1516-1521). IEEE.

[19]. D. B. Johnson, D. A. Maltz, and Y. Hu, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)” <draft-ietf-manet-dsr-09.txt>, April 2003.

[20]. C. Perkins, E. Belding-Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” RFC 3561, July 2003.

[21]. Hu, Y. C., Johnson, D. B., & Perrig, A. (2003). SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad hoc networks, 1(1), 175-192.

[22]. Hu, Y. C., & Perrig, A. (2004). A survey of secure wireless ad hoc routing. IEEE Security & Privacy, 2(3), 28-39.

[23]. Rahman, S. M. M., Inomata, A., Okamoto, T., Mambo, M., & Okamoto, E. (2007). Anonymous secure communication in wireless mobile ad-hoc networks. In Ubiquitous Convergence Technology (pp. 140-149). Springer Berlin Heidelberg.

[24]. Papadimitratos, P. (2006). Secure ad hoc networking.

[25]. Gahlin, C. (2004). Secure ad hoc networking. 1st March.

[26]. Manoj, S. M., & Vasundra, S. An efficient protocol for secure communication in Wireless Ad Hoc Networks.

[27]. Kong, J., Luo, H., Xu, K., Gu, D. L., Gerla, M., & Lu, S. (2002). Adaptive security for multilevel ad hoc networks. Wireless Communications and Mobile Computing, 2(5), 533-547.

[28]. Hu, Y. C., Perrig, A., & Johnson, D. B. (2003, September). Rushing attacks and defense in wireless ad hoc network routing protocols. In

Proceedings of the 2nd ACM workshop on Wireless security (pp. 30-40). ACM.

[29]. Pirretti, M., Zhu, S., Vijaykrishnan, N., McDaniel, P., Kandemir, M., & Brooks, R. (2006). The sleep deprivation attack in sensor networks: Analysis and methods of defense. International Journal of Distributed Sensor Networks, 2(3), 267-287.

[30]. F. Stajano, Security for Ubiquitous computing. John Wiley & Sons, Ltd., 2002.

[31]. F. Stajano and R. Anderson, "The resurrecting duckling: security issues in ad-hoc wireless networks," in Proc. of the Third AT&T software symposium, 1999.

[32]. Banerjee, S. (2008, October). Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. In proceedings of the world congress on engineering and computer science (pp. 22-24).

[33]. Krontiris, I., Dimitriou, T., Giannetsos, T., & Mpasoukos, M. (2007, July). Intrusion detection of sinkhole attacks in wireless sensor networks. In International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics (pp. 150-161). Springer Berlin Heidelberg.

[34]. Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. computer, 35(10), 54-62.

[35]. Hu, Y. C., Perrig, A., & Johnson, D. B. (2003, April). Packet leashes: a defense against wormhole attacks in wireless networks. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies (Vol. 3, pp. 1976-1986). IEEE.

[36]. Alem, Y. F., & Xuan, Z. C. (2010, May). Preventing black hole attack in mobile ad-hoc networks using Anomaly Detection. In Future Computer and Communication (ICFCC), 2010 2nd International Conference on (Vol. 3, pp. V3-672). IEEE.

[37]. Li, Q., Zhu, S., & Cao, G. (2010, March). Routing in socially selfish delay tolerant networks. In INFOCOM, 2010 Proceedings IEEE (pp. 1-9). IEEE.

[38]. Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576.

[39]. Conti, M., & Giordano, S. (2014). Mobile ad hoc networking: milestones, challenges, and new research directions. IEEE Communications Magazine, 52(1), 85-96.

[40]. Liang, C., & Yu, F. R. (2015). Wireless network virtualization: A survey, some research issues and challenges. IEEE Communications Surveys & Tutorials, 17(1), 358-380.