National Conference on Recent Advances in Computer Science and IT (NCRACIT)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 1 | ISSN : 2456-3307

Security Challenges, Threats and the Countermeasures in Mobile Ad hoc Networks: A Review

Samia Khan[1]

[1]Department of Computer & Communication systems, Faculty of Engineering, Universiti Putra Malaysia (UPM), Serdang, Selangor Darul Ehsan, Malaysia

ABSTRACT

A moveable network is self-configurable network in which moveable nodes message with each other with the help of wireless connections without any specified environment. MANETs are becoming a widely known technology for delivering pervasive computing environment. There has been a rapid growth in the adoption of MANETs over last few decades for providing the smart environment. With all these advancements, comes the issue of security in MANETs. The security is a big issue and the chances of having susceptibility to various attacks. It analyses the effects of black hole attacks on the network evaluation. This paper reviews the impact of Blackhole Attacks in Mobile Ad Hoc Networks and various countermeasures for this type of attack.

Keywords : Mobile Ad hoc Networks, Black hole attacks, Security Attacks.

I. INTRODUCTION

Mobile Ad hoc Networks are emerging technologies and their future is appealing. These networks give the clear vision and hope of cheap, anywhere, all time communications that are not physically wired. There has been an increase in the diversity and types of computers with the recent advancements of technology. MANETS is an emerging area of research that include social, technical, the network which contains embedded technologies like devices, humans, vehicles, buildings, connected with the embedded electronic and sensors[5]. The devices are overcoming the number of the user shoulder on a planet because of the low data rate and high computation. These networks have advantages and disadvantages as well. The advantage of these systems is that being mobile they communicate with the rest of the globe. And the disadvantage is that they have few limitations and challenges that will be discussed below. The paradigm set by the modern gadgets has completely changed the perception of the current society regarding technology. MANETs have become popular in every field and offered a greater promise in any area. MANETs find a variety of applications in different scenarios from military services to the hospitals. MANETs provide the opportunity for reducing the cost of monitoring, tracking and for other applications because of their short range network, low data rate, etc. [1]. In of the fields, the primary MANETs objectives are to provide a higher level of accuracy, to improve the assistance, reduce the cost and most specifically the privacy and security of data. A large number of devices and systems are now directly getting connected to the cloud, enabling the access to control and manage the persons or things from anywhere. Some modern devices and application of MANETs include security systems, utility components locks, monitoring, smart

agriculture, home automation, lighting, thermostats. [2].

MANETs consists of thousands of sensor nodes which are equipped with actuators, computing and communicating abilities [3] that enable the devices to communicate, hear and perform different jobs without the involvement of the humans. The sensor nodes in these systems have learned to think and play on their own with the chunks of application logic. The network connectivity and the capability for computing extend to the higher level like to objects, sensor devices, and other routine use devices which are not necessary the computers. The sensor nodes [5] are used for various purposes like monitoring, surveillance, weather, energy, sound, etc. In MANETS, the sensor nodes are deployed, and they have the ability to sense the data, collect it and transfer it to the Destination [11]. In MANETS, the nodes are much smaller when it comes to their size, and so much cheaper in price as well. They consist of resource constraint and low-cost sensor nodes that can be deployed across the places with varying size. The sensor devices are embedded with sensors for monitoring the environment. The MANETs are a collection of wireless nodes that, over a shared channel, communicate with each other directly. The sensor node is the most significant component of the wireless sensor network. These components are small, embedded with sensors or actuators. The sensor nodes are powered by the power source like batteries. Sensor nodes are very cheap and are equipped with the wireless communication system.

A sensor node assembles the data from the physical surroundings which then converts the data into digital form and sends the data in the digital form to the destination. In contrast to the sensor node, the base station provides the graphical user interface to interact with other users and also to forward the data which is sensed to the remote server via Internet. A base station has much better memory, computational power, and a better power energy source than a sensor node. Thus they have emerged in a lot of applications for these sensor networks like body sensor networks in health-care, transportation sensor, monitoring of the environment, location tracking, home automation. With all these advancements, sensor networks also provide circumstances to violate security. Data is one of the most sensitive categories, among all the things that we have in our life. If it is shared inappropriately, it has the potential to have pernicious effects, could be fatal for a person and harmful for his reputation or mostly for his job. It's challenging to capture the potential benefits of MANETS and manage all the threats and vulnerabilities. As the adoption rate of sensor networks technology is taking over the hold, the importance of increasing the security of these systems will also increase. With the attention-grabbing MANETS, security cannot be made an option. For the improvement for delivering appropriate services, almost every other sector is adopting MANETs. Parallel to this adoption, the traditional means for exchanging, collecting of data between the wireless sensor devices is the Internet. This raises significant issues and challenges that could come in the way of the potential benefits provided by the sensor network applications. MANETs are more susceptible to the threats compared to the wired networks because of one simple reason; there is no physical access to the network. The attacker can sit anywhere and eavesdropping the secure communication. MANETS's are considered to benefit the people and society in the future. But to keep it beneficial, we must be able to address the security fundamentals correctly. In this survey, we review the security issues on the network layer, and we will focus on the Black hole attack aka packet dropping attack that the sensor devices are facing and the proposed mechanisms to mitigate the attack.

A. Security in MANETS

Securing in wireless ad-hoc network is mainly problem for several reasons including:

- *Susceptibility of Channels:* Message could be eavesdropped and duplicate messages could be injected into the network, with no required of Physical access.

- *Susceptibility of nodes:* Each node could be simple considered and can fall under the control of the hijacker.
- *Absence of infrastructure:* Networks operate self-sufficiently of any infrastructure, which creates in-applicable any solutions based-on authorization authorities and servers.

B. Security Challenges in MANETS

It's quite demanding to address the security in MANETs because of the resource constraints, absence of centralized authority, vulnerable nodes, memory, infrastructure absence of the devices, power. Black hole attacks can affect the performance parameters of the network like, throughput, delay, load balancing, congestion etc..The security of MANETs needs an innovative and new approach to the security. We summarize the challenges in MANETs from [27], [28] as follows:

- *Standard of routing protocols*: Routing protocols for security have been designed for securing the MANETs. These protocols are standardized in order to develop and implement technical standards. Because of the standardization of the security protocols in the network, the protocols are introduced globally. This standardization also makes it easy for attackers to breach the security by knowing the protocols.

- *Lack of Infrastructure:* MANETs work without an infrastructure. This leads to vulnerability to security attacks. Monitoring the data in an infrastructure less network also makes it more difficult without a proper management. With lack of infrastructure, users are allowed to communicate and route the data using intermediate nodes. So, organizing these networks is must otherwise the network could fail.

- *Energy Constraints:* MANETs consist of nodes that are powered with batteries which are small and can't be recharged. This is one of the challenges in MANETs. Batteries usually run out of time. So, design and implementation of these nodes with high efficiency and less power consumption is important.
- *Dynamic Topology:* The nodes in the MANETs are unpredictably mobile in the network. At any time , these nodes can join or can leave the network which specifically will affect the trust status among the nodes present in the network thus leading to the complex routing.

- *No Centralized Monitoring:* There is no central based monitoring for MANETs. In MANETs, the nodes communicate on the mutual trust basis. Based on this trust, the nodes become more prone to the attacks and threats in the network. There is no main centralized system that takes an account of the nodes. So, if the nodes leave or enter the network, there is no main body to watch them joining or leaving the network.

- *Security Mechanisms:* A lot of security mechanisms have been proposed but no proper single technology is proven to be the best one. This is mainly due to the different limitations like in bandwidth, network structure or the coverage. There are no clear defense mechanisms for the attacks in MANETs. This thing has created the circumstances for the MANETs against the security attacks.

C. Basic Security Goals in MANETS

In designing any secure system, these attributes must be protected. The security requirements are the same whether it is the MANETs, WSNs, VANETs or fixed networks. Because of the inheriting characteristics of the MANETS, they are more vulnerable to the attacks [5]. Also, due to the open access and exposure of nodes and channels to the adversaries,

dynamism of topology, lack of infrastructure, implementing security is quite a challenge.

- *Data freshness*: This is one of the most significant attribute of data quality in MANETs. Data freshness makes sure about the freshness of data that means the data is fresh. It makes sure that no attacker has modified or replayed the original data. Freshness are of two types. One is weak freshness which is needed in sensor measurements, and the other is strong freshness that is needed for synchronizing time in MANETs.

- *Data Authentication*: In sensor networks, data authenticity is much important. Authentication means confirming the truth about the data which a node claims to be true. This assures the source of information and identifies the origin of data. Authentication is special case of integration. Data authentication helps in verifying that the data is really from the desired source.

- *Data Availability*: Availability, as is clear from the name means the presence of data when needed. If right people access the data on right time, then only the information is valuable. Usually DOS (Denial of Service) attacks limit the access to the data or the resources. The authors in [17] have addressed the data availability to a great extent recently.

- *Data Integrity*: It is the prevention of the changes that are not authorized. Data integrity makes sure that the data which is being transmitted has not been modified by the attacker. Data integrity fortifies that the data is not rephrased by any third party either deliberately or accidentally. Data integrity also includes the source or origin integrity which means the data came from the actual source and not from an adversary.

- *Data Confidentiality*: When we use word confidentiality, we mean preventing data from the unauthorized access. Data confidentiality means to conceal the data. Data confidentiality limits the access to the information. Data confidentiality prevents the data from being accessed by the unauthorized users and it lets the access to data by the authorized users only. Confidentiality also is an important part of security. In [18], the researchers addresses the data confidentiality using their propose approach.

II. LITERATURE REVIEW

Simranpreet Kaur et al., 2015 [4] defined network where nodes could act as hosts as-well-as routers. MANETs could be functional in military, release system and worldwide used. Various security issues regarded to MANETs since of its dynamic topology, power-constraint of mobile nodes which create security of this networks significant research area. MANETs are vulnerable to various attacks like wormhole attack, black hole attack and jellyfish attacks. Jellyfish attack is denial of service attack which is dissimilar to detect as it observes all the procedure rules. Major focus is on jellyfish attack and its detection and prevention methods.

Pooja et al., 2015 [6] study three movement models of one-simulator for mobility is completed and then choose the best model. Here hint based probabilistic routing protocol is used to implement a local-utility function based method to detect black-hole using different performance metrics like packet drop and overhead-ratio in the network.

M.Rmayti et al.,2014 [7] proposed a new approach of watch-dog based on two Bayesian Filters: Bernoulli and multinomial. They use these binary models in a complementary manner to successfully detect an information lack attacks in moveable networks.

Anjali Sardana et al.,2015 [8] defined as a collection of various movable nodes which creates a temporary network. In black hole could be defined as a attacker node which on any request of path replies in an in-correct manner as if it has novel path to the goal and

then it drops all in-coming packets. Drop will be very high if malicious nodes work collectively. It gives the analysis of black hole attack –AODV protocol performance by frequently modifying black hole nodes.

Ajay Vikram Singh et al., 2015[9] described the mobile ad-hoc network change of interval, technology has also been evolving, due to this technology has modified from the fixed wire to the probability aspect. MANETs is a collection of cellular infrastructure less mesh topology of the mesh modifies continuously. The traditional security explanations were in-adequate, hence security shall be maintained all levels.

Table no. 1 Limitations in attack

Types Attack	Demerits
Black Hole attack	Network traffic is absorbed
DDos attack	Packet forwarding misbehavior and violate the security

III. ATTACKS ON DIFFERENT LAYERS

The third party can easily hack the Manets devices, most of the times are not designed with the cyber security in mind, and hence the software run by these devices, and the data can be easily compromised and changed unexpectedly. The fact that they are making security an afterthought is the competition demands the manufacturers to launch the hardware product quickly in the market. the attacks can be at different layers like physical layer, transport layer, network layer, link layer [16].

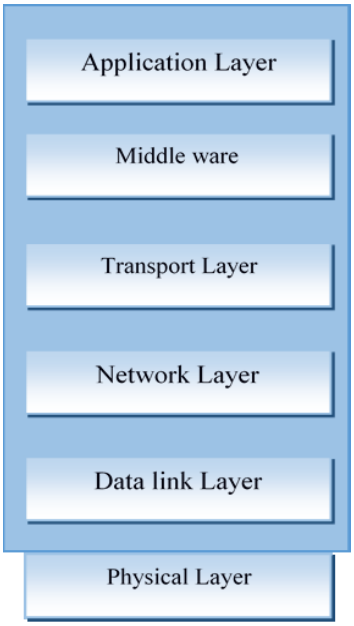

Figure 1. Model for sensor networks

A. Physical Layer

This layer works with the networks physical aspects. It deals with frequency generation, selection, modulation of signal, detection [17].This layer is easy to deal. The Physical layer is used for transmission of data, reception of data for signaling, encryption, etc. This layer deals with the physical connections on a network. Attacks on this layer are as:

- Tampering.
- Jamming.

B. Data Link Layer

This layer deals with the addressing of MAC (Medium Access Control), and also it deals with the VLAN. This provides the node to node delivery for data and the flow control. In this layer controlling of error is done. It helps in assembling the data frames. Attacks on this layer are:

- Exhaustion Attack.
- Unfairness Attack.
- Denial of Service Attack.
- Collision Attack.

C. Transport Layer

The transport layer is used for delivering and receiving of data, working transparently with the other layers. The logical connection running on different hosts is provided by the layer of carriage

between application processes and the other components of a network within an architecture of protocol. Services furnished by the transport layer are the integrity of the data, multiplexing, flow control, etc. Attacks on the transport layer are:

i. *Desynchronization attacks:* In this attack, the attacker sends the fake packets between two sensor nodes, and intrudes the working link. These attacks can be failed by authenticating the whole packet or by authentication of the packets header. In this attack, the attacker changes the sequence number which leads to the de-synchronization of the nodes. By this, the sensor nodes energy is wasted by retransmitting the data.

ii. *Session Hijacking*: In this attack, the attacker secretly takes the session ID of the user. The attacker pretends to be someone known and accesses the data. Most communications are secured at the initial session setup by the credentials and not after that; the attackers usually take advantage of this fact in the connection. This attack falls into three types: Blind hijack, Man in the middle, Session theft.

iii. *Flooding attack:* It's the UDP flooding attack. UDP is a connectionless protocol. This attack floods the server by sending a lot of countless requests to the server. With this weird behavior from the attacker, the server thinks that the user (attacker) needs the service urgently, and it provides services to the attacker. Due to this, the actual users get overlooked. Also, the attacker sends many requests to the target node for establishing the connection and with doing this; it exhausts the resources of the destination node.

D. Network layer

This layer controls the sub netting operation. Based on the network condition and some other factors, this layer decides which path the data should select. This layer provides, fragmentation of frames, controls subnet traffic, provides routing, translates names or the logical address into the physical addresses. The attacks on this Layer are:

i. *IP Spoofing:* First of all, in this attack if the attacker has the sequence number of the targeted host, then the attacker can only attack. Because establishing the connection before attacking is important. If the attacker doesn't have the sequence number of the targeted host, the attacker can't establish a connection and hence can't make an attack on a host. In this attack, the attacker uses a different IP address like of another host. The attacker communicates with the target host using that IP address. The target host is not identified about the attack and the host replies and responses back to the attacker. One more thing about this attack is that if the destination host is active, the attacker can attack the host until then, and if it's inactive the attacker can't attack the host.

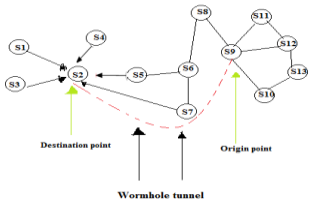

Figure 2. shows the IP Spoofing attack

ii. *Wormhole Attack:* The adversary creates a passage in a network. The adversary pulls down the data packets at one location, sends it to the tunnel and then retransmits the manipulated data from the tunnel to the network. This attack can be a serious threat to the sensor network. This attack can exploit the routing by transferring the information to an undesired destination rather than the original one.

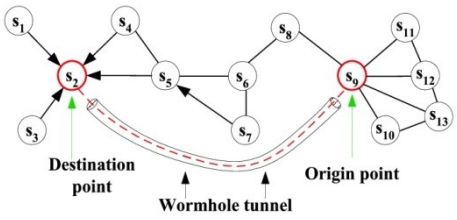

Figure 3. Wormhole attack

iii. *Sybil Attack:* As evident from the name, the attack is given the name from the subject of the book "Sybil" in which a woman suffers multiple personality disorder. This attack can break down the one-way security in a network. In this attack, the node claims to have multiple identities. So, the attacker with the multiple identities will either disrupt the information or it will steal it. With this fake identity of the node, the attacker violates the routing algorithms of the network.

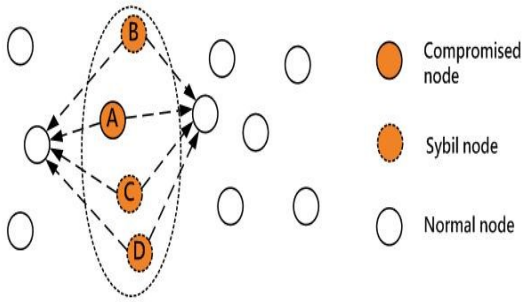

Figure 4. Sybil Attack.

iv. *Black hole Attack:* This type of routing attack can cause harmful effects in the network[15]. The adversary reprograms the node and tries to stop the packets from being transmitted to the destination. With the result, the information that is supposed to be delivered to the base station is captured by the malicious node. The black hole attacks undermine the effectiveness of the network. They have the capability to divide the network so that the useful information would not reach the destination. A black hole attack is a form of Denial of service attack. These black holes are difficult to discover and prevent. In [19], the researchers have explained in detail about the black hole attack.

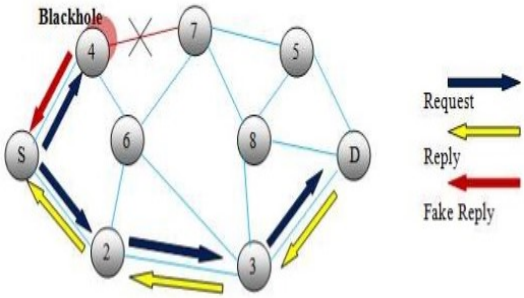

Figure 5. Black Hole Attack

IV. CRYPTOGRAPHIC TECHNIQUES

These techniques that must be development in the Wireless Sensor Network must confirm all the cryptographic needs. Sensor nodes drops in the resource restrictions such as memory capabilities and computational.

i. *Symmetric Technique:* This algorithm adds a class of methods for cryptography that uses similar key for the aim of encryption of plain-text and decryption of chiper-text. The famous symmetric cryptographic methods include blowfish, AES, DES and IDEA [10].

When expending Symmetric techniques, similar-key is used for decryption and encryption by both the parties.

ii. *Asymmetric Technique:* This technique also called as public-key cryptography, two mathematically connected keys and employed. Normally, the decryption key is kept secretly, therefore called as 'Private Key' and 'Secret key', while the encryption key is known as 'Public Key' because it is range to everybody those who may require to send the encrypt message. If it is possible for someone used public-key to send the encrypted messages to the owner of the private key. The private key couldn't re-build from the public key. Various types of asymmetric key are ELGAMAL, RSA and ECC etc[12].

Table II Difference between Symmetric and Asymmetric Encryption Techniques

Symmetric Approach	Asymmetric Approach
Uses the similar-key to together encrypt and decrypt	Uses single key to encrypt and dissimilar one to decrypt.
Commonly used symmetric encryption techniques include DES, 3DES and AES are commonly used in IPec.	Asymmetric algorithm is RSA, Elgamal, ECC [13].
Extremely Fast and their relatively less complexity allow for easy implementation in H/W.	More secure since it relies on digital documents.[14]

Table III Comparison various Approach

Features	DES	RSA
Key used	Same key is used for encryption and decryption	Different Keys are used for encryption and decryption Purpose
Scalability	It is scalable algorithm due to changing the key-size / block size	No scalability occurs.
Avalanche effect	No more effected	More effected
Throughput	Low	High
Confidentially	High	Low

V. CONCLUSION

We observed that a lot of active research is being done in this area, and it is still in its early stage. The proposed techniques are not absolute solutions regarding efficient and effective security. The security in the MANETs needs much more attention. The absence of fixed infrastructure, dynamic topology, weak channels and nodes, limited capacity for computation, limited battery life/power are the primary limitations of the MANETs. These restrictions make the implementation of the security a little difficult in these networks. Therefore, an ambitious goal for MANETs is to develop a practical solution for security that results from the in-depth protection that offers good defense against black hole attack as well as DDOS attacks while discovering the network. We analyzed that the security schemes implemented for detecting and preventing black hole attacks degrade performance somehow. We reviewed that the use of asymmetric keys for securing MANETs did not prove to be an efficient approach. Most of the research done on black hole attacks in MANETs has put efforts on mitigating the attack present in the network after the route discovery process. So these security mechanisms implemented for detecting and preventing the black hole attacks consume more processing power, computational capacity, are slow which makes them not much feasible for MANETs. We propose, an approach, using P-Shape Encryption Techniques to secure the packets. It will efficiently detect the attacks before route discovery.

VI.REFERENCES

[1] Wang, Fei-Yue, and Derong Liu. "Networked control systems." *Theory and Applications, Springer-Verlag, London* (2008).

[2] Halim, Tasneem, and Md Rafiqul Islam. "A study on the security issues in WSN." *International Journal of Computer Applications* 53, no. 1 (2012).

[3] Oh, Jong-Ha, Sung-Sik Jang, and Tae-Young Byun. "A Centralized Cluster Head Selection Scheme for Reducing Discrepancy among Clusters over WSN." In *Embedded and Multimedia Computing Technology and Service*, pp. 699-706. Springer Netherlands, 2012.

[4] Kaur, Simranpreet, Rupinderdeep Kaur, and A. K. Verma. "Jellyfish attack in MANETs: A review." In *Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on*, pp. 1-5. IEEE, 2015.

[5] Chauhan, R. K. "An assessment based approach to detect black hole attack in MANET." In *Computing, Communication & Automation (ICCCA), 2015 International Conference on*, pp. 552-557. IEEE, 2015.

[6] Rmayti, M., Youcef Begriche, Rida Khatoun, Lyes Khoukhi, and Dominique Gaiti. "Denial of service (DoS) attacks detection in MANETs using Bayesian classifiers." In *Communications and Vehicular Technology in the Benelux (SCVT), 2014 IEEE 21st Symposium on*, pp. 7-12. IEEE, 2014.

[7] Sardana, Anjali, Tushina Bedwal, Akanksha Saini, and Radhika Tayal. "Black hole attack's effect mobile ad-hoc networks (MANET)." In *Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in*, pp. 966-970. IEEE, 2015.

[8] Singh, Ajay Vikram, and Moushumi Chattopadhyaya. "Mitigation of DoS attacks by using multiple encryptions in MANETs." In *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2015 4th International Conference on*, pp. 1-6. IEEE, 2015.

[9] Kumar, Sandeep, and Suman Sangwan. "A Survey of Black Hole Detection Techniques in WSNs." International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 5, May 2015.

[10] Sasi, Swapna B., Dila Dixon, Jesmy Wilson, and Page No. "A general comparison of symmetric and asymmetric cryptosystems for WSNs and an overview of location based encryption technique for improving security." *IOSR Journal of Engineering* 4, no. 3 (2014): 1.

[11] Bao, Fenye, Ray Chen, MoonJeong Chang, and Jin-Hee Cho. "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection." *IEEE transactions on network and service management* 9, no. 2 (2012): 169-183.

[12] SenthilKumar, U. SenthilKumaran1 MK Nallakaruppan2M, and U. Senthilkumaran. "Review of asymmetric key cryptography in wireless sensor networks." *International Journal of Engineering and Technology* 8, no. 2 (2016): 859-862.

[13] Watro, Ronald, Derrick Kong, Sue-fen Cuti, Charles Gardiner, Charles Lynn, and Peter Kruus. "TinyPK: securing sensor networks with public key technology." In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, pp. 59-64. ACM, 2004.

[14] Aman, Kumar, Jakhar Sudesh, and Makkar Sunil. "Comparative Analysis between DES and RSA Algorithm." *International Journal of Advanced Research in Computer Science and Software Engineering* 2 (2012): 386-389.

[15] Baadache, Abderrahmane, and Ali Belmehdi. "Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks." *arXiv preprint arXiv:1002.1681* (2010).

[16] Akyildiz, Ian F., Weilian Su, Yogesh Sankarasubramaniam, and Erdal Cayirci. "A survey on sensor networks." *IEEE Communications magazine* 40, no. 8 (2002): 102-114.

[17] Kamra, Abhinav, Vishal Misra, Jon Feldman, and Dan Rubenstein. "Growth codes: Maximizing sensor network data persistence." In *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 4, pp. 255-266. ACM, 2006.

[18] Bajaj, Sumeet, and Radu Sion. "Trusteddb: A trusted hardware-based database with privacy and data confidentiality." *IEEE Transactions on Knowledge and Data Engineering* 26, no. 3 (2014): 752-765.

[19] Tamilselvan, Latha, and V. Sankaranarayanan. "Prevention of blackhole attack in MANET." In *Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on*, pp. 21-21. IEEE, 2007.