IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 5, May 2017

Survey: Security Attacks in Wireless Sensor Networks

Salima Rashid Al Dhabooni[1], Hothefa Shaker Jassim[1], Zeyad T. Sharef[2], Baraa T. Sharef[3]

Modern College of Business and Science, Al-Khuwair, Oman[1]

College of Engineering, Ahlia University, Manama, Bahrain[2]

College of Information Technology, Ahlia University, Manama, Bahrain[3]

Abstract: Many objects around us are placed on a network via wireless sensor network (WSN). This type of network is considered new technology and it begins to grow and raised in order to allow data to be stored, processed and accessed in an efficient way. It is used for observing, checking, or keeping a continuous recording of a process or quantity of ecological circumstances such as heat range, audio, pressure and wetness to hand in glove successfully go their data over the network to specific location . The difficulty in WSN network is that the network access is not secure or not safe when data transmits through wireless environment. It is susceptible to assault and intruders. Additionally, denial of services attacks much more damaging. Security issues are biggest issue in the field of wireless sensor networks. This paper focuses on looking at the current safety troubles of wireless sensor networks and recommended suitable controls to triumph over these problems.

Keywords: wireless sensor networks, security issues, intruders, denial of service.

I. INTRODUCTION

A wireless sensor network is considered as one type of networks that contain large or huge numbers of sensor nodes. In other words, it comprises of spatially allocated independent receptors that are called sensors. Sensor nodes are little in size, less storage, less expensive in cost with limited source of energy and constrained in ability of processing WSNs are quickly becoming more popular because of minimal effort solutions to a range of real life difficulties [1] [2].
Many domains have adopted WSN for example: military, monitoring, transportation, health, industry, ecological circumstances, etc[4].The essential thought of sensor network is to spread or scatter small sensing devices that are equipped for detecting a few changes of occurrences or factors and interacting with another device over a particular geographical range for a few certain functions such as observation, ecological checking, target following and so forth.
One of essential objectives for Wireless Sensor Networks (WSNs) is to gather data from the physical world. In addition, the features of using wireless sensor networks are contrasting with current infrastructure – primary based networks, WSNs have the ability to work in any surroundings and anywhere, so appropriate for the places that we cannot reach it easily, for example, over the ocean, mountains, rustic ranges or profound woods. It prevents a lot of cabling or wiring and easy to use. WSNs are usually implemented to sense, process and spread data of targeted actual surroundings[2][10].This paper discusses the security problems specifically attacks that experiencing current wireless sensor network and possible solutions to these problems according to different groups ideas.
The remainder of the paper is structured as follows: Section II, explains the general definition, description and structure of the wireless sensor networks. Section III, provides a fundamentals of security principle. Next section, presents the security threats based on the most recent studies. Last part presents the analysis and discussion of the research.

II. DESCRIPTION OF WIRELESS SENSOR NETWORKS (WSNS)

Wireless sensor networks described in [10] as a substantial technology utilizes low-power, low-cost and multi-functional tiny sensors that communicate in short distance. Smart sensors are not expensive and communicate with each other through wireless links positioned in large numbers in different locations to monitor and control different domains. Sensor nodes are little in size, less storage, less expensive in cost with limited source of energy and constrained in ability of processing [22].

III.OVERVIEW OF WIRELESS SENSOR NETWORKS ARCHITECTURE

As shown in Figure 1, the WSN is a number of sensor nodes distributed in receptors place that gather and direct data back to the bottom place. A sensor node is divided into four essential areas: the indicator device (sensing), process device, transceiver device and energy source device. Localization is one heart of the course plotting idea in WSN. The

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

position finding system assists the sensor node to find its place within the establishing. The energy device could be the source of energy to the sensor nodes that is the main concentrate on place of the scammers [6] [16].

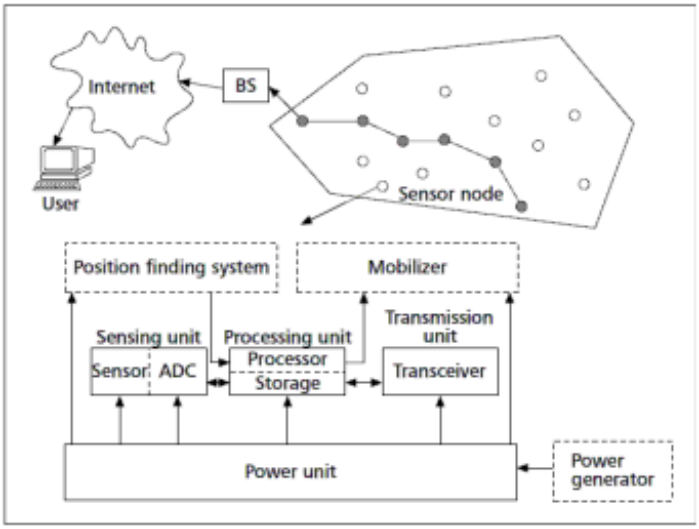

Fig.1: Wireless Sensor Network Architecture

Generally, the wireless sensor networks are used widely due to the availably of micro-sensors and low-power communication. Most of WSN structure contains the following components:
1) Sensor motes: field devices that are capable of routing packets along with other devices.
2) Gateway or Access points: a device that enables the communication between the field devices and applications.
3) Network manager: a device that is responsible of the configuration between the devices for example: network health and routing tables.
4) Security manager: a device that is responsible of generating, storing and managing keys.
A wireless sensor node as seen in Figure 2 is attached with sensing and computing equipment's, radio transceiver and energy modules. WSN is a technology that inherits popularity because of the flexibility associated with it while solving many problems [11] [3] [17].

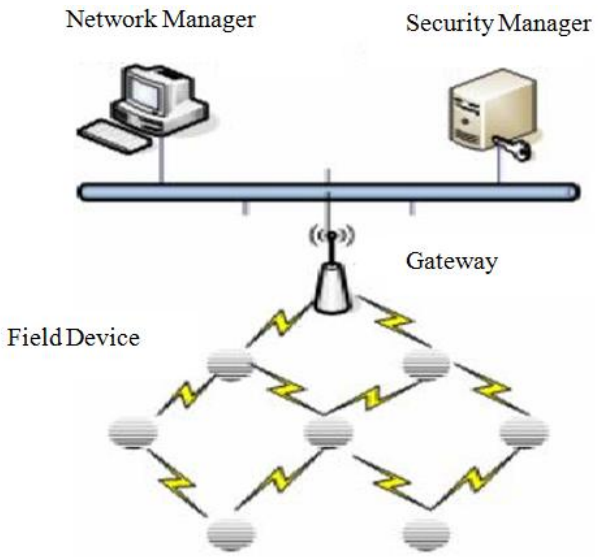

Fig.2: Wireless Sensor Nodes

IV. FUNDAMENTAL PRINCIPLES OF SECURITY

In general, security is related to these four aspects: Confidentiality, Integrity, Authentication and Availability (CIAA) [5].

A. **Confidentiality:**

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

It is like privacy capable of disappearing information from an inactive attacker so that any concept conveyed via the sensor system continues to be private. This is the maximum critical problem in network safety. A sensor node must not disclose its information to the others who live nearby.

B. **Authentication:**

It is same as verification that guarantees the accuracy of the message by determining its source.So, it is necessary to prove whether the message is actually coming from its source or not.

C. **Integrity:**

It means the ability to emphasize the message which has not been modified. In other words, it relates to the capability of assuring that the concept has not been interfered or modified while it was on the network. An attacker is not just restricted to changing the data packet. It can modify the whole bundle flow by injecting additional packages. Thus, the recipient needs to make sure that the data used in any decision-making procedure starts from the correct resource. The integrity of the system will face a problem when:

• Harmful node is available in the network that inserts incorrect information.
• Volatile conditions because of wireless route causes destruction or loss of information [9].

D. **Availability:**

It is presented when a node can utilize the resources and the network should be available 24 every 7 days for a message to connect. Availability is necessary and there must be no failure in the network in order to perform the functions.

V. SECURITY PROBLEMS IN WIRELESS SENSOR NETWORKS

Wireless networks are at risk of security attacks because of the published nature of the transmission medium or the way of communication of the transmitting method. Moreover, WSNs have an extra weakness due to nodes are usually placed during a threatening or hazardous surroundings wherever they are not physically secured.

Many researchers have discussed security and privacy issues of wireless sensor networks. Thru literature evaluations of recent security problems of WSNs, the current research is capable of integrating some problems that authors have outlined in WSN. In addition, the main contribution of this study is to classify the recent issues that depend on capacity of attackers, attacks of records in transmission and based on network layers [10].Before going further to define types of attacks, let's explain the main and common kind of attack that is recognized as Denial of service (DoS). It is harmful action causes Refusal of Support. During transmission more repetitive packages, the simplest DoS strike efforts to consume the sources obtainable to the sufferer node. As a consequence, it restricts legal clients in system from getting entry to services or sources to which they are eligible DoS strike is meant to the scamper's try to damage or destroy a system, and furthermore for all activities that decrease a network's capability to set up a service [15]. Here we point out the common types of attacks in wireless sensor networks [22].

A. **Based On the Capability of the Attacker:**

Outer compared to inner attacks: the outer attacks are originated from a node that is not part of a WSN. Inner attacks may bring inactive listening in information transmissions and in addition can increase providing fake information into the network to expend the network sources and lift refusal or denial of service. On the other hand, the inner attacks happen when genuine nodes of a WSN act in random or illegal methods. Inner attack is an approved member in the sensor system that looks for affecting functions or manipulates business resources. To get over these attacks, we need strength or hardiness against outer attacks, flexibility to inner attacks as well as Genuine Levels of Security[2][10].

Passive compared to active attacks: Inactive attacks involve observation-tracking packages interchanged within a WSN while active attacks include a few alterations or some modification of the data flow or the creation of the wrong flow [1][4] [5] [11].

Mote-class compared to laptop-class attacks: In mote category, an attacker strikes a WSN by utilizing little nodes through identical abilities as that of system nodes. In laptop-class strikes, an attacker can utilize better devices for instance laptop as well as can do extra damage to a system than a harmful indicator node. These devices have an increased transmitting range, and energy source than the system nodes [10].

B. **Attacks on Data in Transfer or passage:**

In a sensor or system, receptors observe the changes of particular values and then report back to the sink consistent with the need. Whereas sending off the report, the data in transit could also be changed, modified, spoofed, replayed once more or disappeared. A wireless interaction is insecure to spying, attacker can observe the traffic or movement circulation and get into action to Disrupt, block, alter or create bundles in this manner, give wrong data to the base stations.

C. **Based on OSI layers:**

Physical Layer

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

Jamming attacks: one of the most significant strikes at physical part, seeking at disrupting normal functions. An opponent may consistently transfer radio alerts on a wireless route. An opponent can send high-power alerts in order to effectively stop wireless medium and to prevent indicator nodes from interaction. To be protected against this attack, spread range methods are used for radio connection. Taking care of sticking over the MAC layer requires Admission Control Technique. Algorithms that merge mathematically examining the received signal strength indicator (RSSI) values, the average time required to sense an idle channel (carrier sense time), and the packet delivery ratio (PDR) methods can effectively recognize all four types of jamming [7] [19].
Tampering: an enemy can draw out delicate information such as cryptographic important factors or other information on the node. An affected node makes, which the enemy manages by changing or changing node. Weaknesses of this strike is logical. One protection to this strike includes tamper-proofing the node's actual package. In other words, an assailant can remove delicate data, for example, cryptographic keys or other information on the hub. Self-Destruction or damage itself whenever somebody accesses the indicator nodes actually the nodes vaporize their storage material and this stops any leak of information. One more is Fault Tolerant Protocols method that is intended for ought to be flexible to this kind of attack [10][13][8].

Data Link Layer
Exhaustion: Harmful node interrupts the Media Accessibility Management method, by consistently inquiring or transferring over the route. This gradually brings a hunger for other nodes in the system about route access. An action is taken to counteract a danger or threat is rate restricting to the MAC entrance control such that the system can neglect extreme demands. Thus, avoiding the energy strain due to recurring signals. A second technique is to use time department multiplexing where each node allocates a moment port in which it can transfer.
Collision: An accident happens when two nodes make an effort to transfer on the same regularity at the same time. When packages conflict, a change will likely happen in the information section, resulting in a testing mismatch at the getting end. The bundle will then be removed as incorrect. A common protection versus crashes utilizes of correct error code (mistake solving codes).
Unfairness: Iterative application of these accident based MAC part attacks or a violent use of supportive MAC part concern systems, can lead to unfairness.
Interrogation: It misuses the two paths that are requested to send and clear to send handshake that numerous mandatory access control protocols utilize to minimize the hidden node issue. An attacker can consume the resources of node by over and again sending RTS messages to evoke (clear to send) reactions from a focused on neighbor node [13][14][18].

Network Layer
Sinkhole: The objective of attacker in a sinkhole strike is to entice almost all the traffic from a special system by way of an affected node, creating a metaphoric sinkhole with the attacker at the bottom place. Normally, by creating an affected node that is seemed to be particularly exciting to encompassing nodes concerning the redirecting criteria, sinkhole strikes can act. Through sinkhole strike, the enemy attempts to entice almost nearly all the traffic from a selected place through an affected node. An affected node which is placed in the middle of some places makes a large "sphere of influence", gaining all traffic intended for BS from the indicator nodes. The enemy objectives a place to make sinkhole where it can entice the most traffic, possibly nearer to the BS so that the harmful node could be considered a platform place or BS [14].
Sybil Attack: A node can occupy several identities that result in failing of the redundancy techniques of allocated information storage networks in peer-to-peer networks Sybil strike features by its property of comprising several nodes at the same time. The Sybil attack is capable of destructive other mistake resistant techniques such as difference, multi path redirecting, redirecting methods, information gathering or amassing, voting, reasonable source allowance and topology servicing. This attack may also affect the regional redirecting methods, where the harmful node provides several details to other nodes in the network and thus seems to be in more than one site at once [20].
Hello Flood: At the beginning of connection, node has to declare itself to the network by transmitting hello message to their nearby nodes. It also checks or proves the validity of the node that transmits hello message is in the near area. Attacker can manipulate this feature by utilizing a powerful wireless connection. It can guarantee each node in the network is its neighbor. In this way the interaction is achieved between nodes. As apparent, by using this strike security of the details is affected as the attacker benefits the accessibility of the circulation details in the system. If the nodes provide accessibility, any node inquires for relationship use some challenge plan, and then a version of this strike can also be provided. Verification is the key remedy to this type of attack. Such attack can easily be ignored by confirming bi-directionality of communication before acting based on the information obtained over that communication [10].
Selective Forwarding: A redirecting node has a primary responsibility that is sending packages. However, any bundle could be decreased and a harmful node might submit other ones deliberately. A failed recognition structure to identify the particular sending strike is by Wang et al. The quantity of packages that must be ahead should be same to the quantity of packages that it gets and it is monitored for a redirecting node. Each sensor node can work under illegal way in their structure therefore; it can overhear the transmitting of nearby nodes. The neighbor is able to work with others

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

living nearby of the alleged node. A choice of the alleged node is designed through collecting the guidelines from the alleged node's others who live nearby, on the situation that neighbor of an alleged node finds going above a particular limit in the bundle variety which failed to be ahead by the alleged node. [14].

Spoofed, Changed, or Replayed Routing Information: This is the most widely recognized direct assault against a redirecting method. This assault mostly focuses on the redirecting details interchanged between the nodes. In order to affect movement in the network, an enemy may spoof, modify or reply redirecting details. These interruptions include the creation of redirecting circles, increasing and reducing source tracks, gaining or rejecting network movement from select nodes, dividing the network, creating fake mistake messages and expand end-to-end response time. Verification is the effective defense measures for these assault i.e. routers will only approve redirecting details from legitimate routers [20] [21].

Transport Layer:

Flooding: An attacker may continuously and more than once make new communication demands till resources needed via every connection are tired or reach a highest possible restrict. It generates serious source restrictions for genuine nodes. One suggested solution for this issue is to require each linking user to illustrate its dedication to the connection by fixing a challenge. As a protection against this class of strike, restriction can be put on the quantity of connection from a specific node.

De-synchronization Attacks: the foe or the attacker continuously over and again forges or spoof information to one or both end host. Subsequently, these messages are again passed on and if the attacker keeps an appropriate moment, it can avoid the end and loose synchronization. A conceivable solution for this attack is to need or request authentication of all packets such as control area between hosts [13].

Application Layer:

Overwhelm attack: An assailant might tries to confuse network nodes together with sensor stimulating elements, resulting in the network to transmit huge amounts of movement to a base terminal or BS. This assault expends the network data transfer usage and empties node power [14].

VI. ANALYSIS AND DISCUSSION

The literature review reveals the concept of wireless sensor network in general. In addition, it provides an overview of the faced issues in the area of network layers. Moreover, a number of techniques have been discussed from different researchers' point of view. Based on the analysis done in the literature review, each issue has potential solution referred as preventive techniques in this paper. Each issue has been mapped against a potential prevention technique, which could help in reducing the risks associated with the issue or avoiding it.

Table 1: Mapping between wireless sensor networks attacks and prevention techniques

Layer	Attacks	Countermeasures
Physical layer	Jamming	Usage spread spectrum methods [12]
	Tampering	MAC for admission control technique
Data link Layer	Exhaustion	Rate Limiting to the MAC admission control and time division multiplexing
	Collision	Solving error code [12]
	Unfairness	Small frame
	Interrogation	Anti-replay security and powerful connection -layer verification or confirmation
Network layer	Sinkhole	Redundancy, key Management
	Sybil	Authorization, Monitoring, Key Management
	Hello Flood	Authentication, packet leashes by geographical and temporal info
	Selective Forwarding	properly adjusting receptors
	Spoofed, changed, or replayed routing information	Egress filtering, authentication, monitoring
Transport Layer	Flooding	Client puzzles [13]
	De synchronization	Authentication [12]
Application Layer	Overwhelm	Rate-limiting and efficient data-aggregation [12]

The above table summarizes the mapping between the issues related to the wireless sensor network issues and the controls that can solve them. The below points are explaining how Table 1 was created and summarized:

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 4, Issue 5, May 2017

- One technique in protecting versus the jamming strike is to define which part that jammed in sensor network. In addition, usage spread spectrum methods for wireless connection.
- To deal with tampering strikes, nodes may implement or utilize a MAC admission control. This would permit the system to neglect those demands intended to consume the power supplies of a node.
- An action taken to counteract to exhaustion strike is amount restricting to MAC admission control such that the system can neglect extreme demands. Another method is to utilize time division multiplexing where every node is designated a period aperture in which it is able to send [12].
- The main protecting evaluation against such strikes is the use of tiny frameworks, so that any individual node grabs the route for only a short period [12].
- To get rid flooding in transport layer, authors in [12] recommend utilize client puzzles in an attempt to recognize a node's involvement or obligation to create communication with the use of some of their own sources.
- Implement key control or key management that aims at setting up the correct keys between nodes in a protected and efficient or trustworthy way in these types of attacks (Sinkhole and Sybil).
- The main important thing in order to protect or secure wireless sensor network from a criminal is by applying cryptographic method that contains encryption and authentication. There are two kinds of cryptography methods that are symmetric and asymmetric. Symmetric encryption means that both of sender and receiver must use same key. The second type is asymmetric in which a sender encrypts the message or information by public key and receiver decrypts that information by his own private key. So two different keys should be in this method. However, unfortunately, it is not possible to apply this method due to a lot of complexity in calculation for each node in WSN.
- Generally, intrusion detection system should be applied to avoid prying or intruder sniffed during communication.

VII. CONCLUSION

The security of WSNs has become an important topic since of the different risks showing and benefit of data privacy, although in the past, there was a little attention to WSNs protection. There are several alternatives to be protected against all risks, although some alternatives have been recommended. In this article, we generally focus on the attacks in WSN protection and the subjective of the WSNs risks that affect numerous levels along with their protection techniques is provided. These days, in place of concentrating on various levels, researchers focus on incorporated system for protection procedure. Therefore, this paper attempted to review some of security attacks and available alternatives that have been recommended by researchers.

REFERENCES

[1] G. Thirumalaimuthu, E. Edwin L. and S. Meenakshi. Security in Wireless Sensor Networks: Issues and. International Journal of Computer Application, 2016.
[2] P. Mahesh, G. Kale, and A.Jaywant. Review: Features, Protocols, Threats and Challenges of WSN. International Journal of Advanced Research in Computer Science and Software Engineering, 2016.
[3] M. S.Manshahia. Wireless Sensor Networks: A Survey. International Journal of Scientific & Engineering Research, 2016.
[4] P. Tiwari, V. P. Saxena, R. G. Mishra, and D.Bhavsar. Wireless Sensor Networks:Introduction, Advantages,Applications and Research Challenges. HCTL Open International Journal of Technology Innovations and Research (IJTIR), 2015.
[5] K. CHELLI. Security Issues in Wireless Sensor Networks: Attacks and Countermeasures. Proceedings of the World Congress on Engineering, 2015.
[6] P. R. Ayachit and N. G. Narole. Security Issues Threats and Challenges in Data Management of Wireless Communication & Sensor Network over Cloud: A Review. Journal of Engineering Research and Applications, 2014.
[7] S.Alam ,and D. Debashis. Analysis Of Security Threats In Wireless Sensor Network. International Journal of Wireless & Mobile Networks (IJWMN), 2014.
[8] K. W. Al-Ani and H. S. Jassim. Review on Routing Protocols for Mobile Ad-Hoc Network. European Journal of Scientific Research, 2014.
[9] H. Chawla. Some issues and challenges of Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Software Engineering, 2014.
[10] M. Roopak, T. Bhardwaj, S. Soni, G. Batra. Review of Threats in Wireless Sensor Networks. (IJCSIT) International Journal of Computer Science and Information Technologies, 2014.
[11] V. Kumar, A. Jain, and P. N. Barwal. Wireless Sensor Networks: Security Issues, Challenges and Solutions. International Journal of Information & Computation Technology, 2014.
[12] M. Chowdhury, M. F. Kader, and Asaduzzaman. Security Issues in Wireless Sensor Networks: A Survey. International Journal of Future Generation Communication and Networking, 2013.
[13] I. S. Kocher, C. Chow, H. Ishii, and T. A. Zia. Threat Models and Security Issues in Wireless Sensor Networks. International Journal of Computer Theory and Engineering, 2013.
[14] R. Panigrahi, K. Sharma, M. K. Ghose. Wireless Sensor Networks –Architecture, Security Requirements, Security Threats andts Countermeasures, 2013.
[15] M. Teymourzadeh, R. Vahed, S.Alibeygi, and N. Dastanpor. Security in Wireless Sensor Networks: Issues and Challenges. International Journal of Computer Networks and Communications Security, 2013.
[16] N.Dzulkhifli, R. Alsaqour, H. S. Jassim, M.Abdelhaq, O. Alsaqour,and R. Saeed. Network services and applications. International Digital Organization for Scientific Information, 2013.
[17] N. Grang and A. Gupta. Wireless Sensors Network: An Overview. International Journal of Modern Computer Science (IJMCS), 2013.
[18] S. K. Tiong, H. S. Jassim, S. Yussof, S.P. Koh, and D. F. Yap. Electromagnetic-like Mechanism based Routing Protocol for Mobile Ad Hoc Networks. Trends in Applied Sciences Research, 2012.
[19] Z. Sharef, A. Alaradi, and B. Sharef. Performance Evaluation for WiMAX 802.16e OFDMA Physical Layer. Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012. DOI: 10.1109/CICSyN.2012.71.

IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 4, Issue 5, May 2017

[20] B. T. Sharef, R. A. Alsaqour, M. Ismail, and S. M. Bilal. A Comparison of Various Vehicular Ad Hoc Routing Protocols based on Communication Environments. In Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, p. 48. ACM, 2013.

[21] B. T. Sharef, R. A. Alsaqour, M. Ismail, and S. M. Bilal. Comparative Study of Variant Position-based VANET Routing Protocols. Procedia Technology, 11, pp.532-539, 2013.

[22] K. S. AlRasbi, H. Shaker, Z. T. Sharef. Survey on Data-Centric based Routing Protocols for Wireless Sensor Networks. International Journal of Electrical, Electronics and Computers, 2017.