Reliable Routing Mechanism against Distributed Denial of Service Attack to maintain web semantics in Wireless Sensor Networks

Abdulaziz Aldaej

College of Computer Engineering and Sciences
Prince Sattam Bin Abdulaziz University, KSA

Abstract
An effective secure routing protocol is proposed against distributed denial of service attack. These networks are used to fix real world problems by deploying the sensor nodes in antagonistic places to keep the surveillance on motion, temperature, sound, vibrations etc. these nodes are power and memory constraints that makes them vulnerable to network attacks. Thus the network security should be efficient and with least computationally complex in order to save memory and battery drainage. The proposed mechanism scrutinize the nodes and block the malicious node if found attacker node or infected node to maintain the real semantics of web. Intrusion prevention scheme is used to allow selected nodes of the network behave as intrusion prevention system nodes. These IPS nodes operate in their multihop area in the network and keep scanning the hops periodically. Whenever this IPS node senses swift data packet passing other than selected (TCP-UDP packets), the infected node is blocked immediately and this message is send to the legitimate node in order to change the routes. We used network simulator version 2 for the simulation and the proposed mechanism provided better results against DDoS attacks. After we applied the proposed mechanism to the network with infected nodes, the performance parameters have been revamped.

Key words:
DDoS, WSN, Web Semantics, AAODV.

1. Introduction

Wireless sensors are group of specialized sensors and actuators which are integrated into machines, structures, and many other places in environment, and capable of transmitting sensed information to monitor and large scale tracking of physical world with grater details and at large scale [1]. Sensors acquire real time information and transmit it to external systems such as the satellite network and the internet. Applications of these sensor network is going to be versatile, manufacturing units, homeland security, conservation of natural resources, smart cities, and home automation, asset tracking, intelligent agriculture and health care systems etc [2]. WSN is one of the emerging technologies and it technically supports Internet of Things (IoT).

Sensors connected with lead wires and fiber optic cables require significant installation and maintenance cost, wireless Sensor Network (WSN) can eliminate these cost. WSNs are scalable, consumes very less power, and software programmable, data acquisition is reliable and accurate, requires no real maintenance [3].

WSN consist of multiple nodes which counts from few to several hundreds to thousands, nodes connect with each other and perform the given functions: sensing, relaying data and exchanging the data with other networks [4]. A node for sensing is called sensor node, data relaying node is router and data exchanging node is sink node. Every sensor has integrated components: transducer, a microcontroller, a radio transceiver and power supply unit [5]. Transducer generated electric signals for sensed natural phenomena and environmental changes, microcontroller process these signals and stores the output, radio transceiver transfers the data to sink node which in turn connects to external devices and transmit the data to internet [6]. Recent advances in Integrated Circuits and Micro Electro Mechanical Systems (MEMS) provided us single low-cost package with wireless communication and signal processing capability [7]. There are many types of sensors based on type of sensing, temperature, humidity, lightning conditions, pressure etc.

WSN uses IEEE 802.15.4 wireless Personal Area Network Protocol (WPAN), Bluetooth, RFID, Zigbee protocol [8].

Challenges and limitations to be addressed in WSN are same as of wireless network and few are specific to WSN, among those challenges to address are energy efficiency, signal distortion, security, amount of data transmission, maintenance of sensor which are geographically spread across large distance [9]. Energy efficiency is addressed with optimization of hardware and software to consume less energy without compromising the objective of WSN, security mechanisms like public key cryptography are not possible in WSN with limited energy and processing power, on the other hand WSN are susceptible for denial of service attacks, authorization of sensor which can provide information, authentication of sensors,

Manuscript received April 5, 2018
Manuscript revised April 20, 2018

confidentiality such that other devices should not intercept the messages between sensors, and many other issues in security of WSN are to be addressed [10]. Attacks on WSN can occur at different layers.

Physical layer attacks include jamming: interference with radio frequency signals used by sensors and tampering: physical access to the sensor where attacker can extract sensitive information from like crypto keys and other data from the sensor node [11].

Link Layer attacks include collision: when two nodes try to transmit with same frequency at the same time, which can result in collision and change in information transmitted [12], mechanism to deal with collision detection and correction demands more processing power. Exhaustion: with repeated collision can exhaust the resources and lose of energy. Network Layer attacks include sink hole attack where attacker creates a node which depicts itself as next hop in the network by forging network information. Sybil: where one host has more than one identity. Transport layer also faces attacks like flooding and Desynchronization [13].

2. Distributed denial of service Attack

DDoS attack is one of major threats in the modern Wolds internet. The literature of computer networks has demonstrated the impact of DDoS in an efficient manner. The major goal of DDoS attack is to disrupt the services provided by the system by prohibiting the access to the server or machine instead of destabilizing the service itself [14]. These attacks either target bandwidth or connectivity to decline the network capability of providing the specified services. DDoS normally achieve their goal by flooding the target with fake packets that decline its network and processing capability [15].

DDoS is a simple technique but powerful and ruthless to target and harm the modern network resources. It has a DID many to one feature to already existing DOS attack [16]. Thus making its detection and prevention more difficult along with securing its impact. DDoS has not got specific feature that could be used specifically for its detection [17].

Modern networks web semantics describe the availability of recourses and services at the end user level with relatively efficient and reliable but DDoS attack can be one problem that may make it difficult to maintain the web semantics of modern networks [18]. DDoS attack is a ruthless attack that is launched to stop or decline the quality of service provided by the system. These attacks do not damage data directly but make the resources and other nodes to compromise [19].

To launch a DDoS attack, an attacker uses a group of coordinative compromised nodes to attack one or groups of targets. The DDoS attacker enhances the effectiveness of the attack using client hewer technology by controlling the resources of group of unaware and unwilling nodes which later serve as attack roots and sources [20]. A typical DDoS attack is comprised of basic four elements as shown in Figure 1.

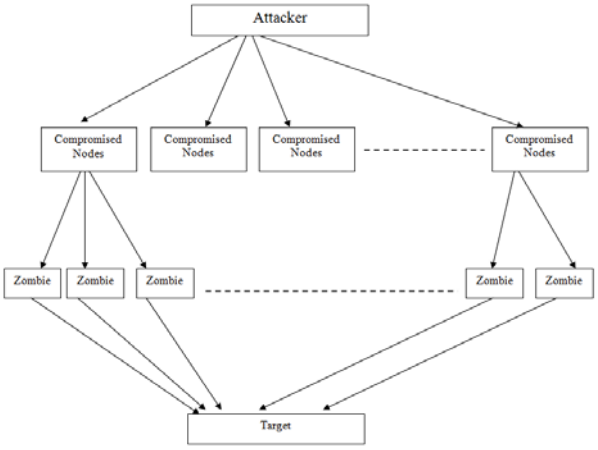

Fig. 1 DDoS Attack architecture and its key elements.

A. source attacker

B. Compromised nodes (Handler)

C. Zombie Hosts (Agent)

D. Target

A DDoS attack can be described as shown in Figure 2

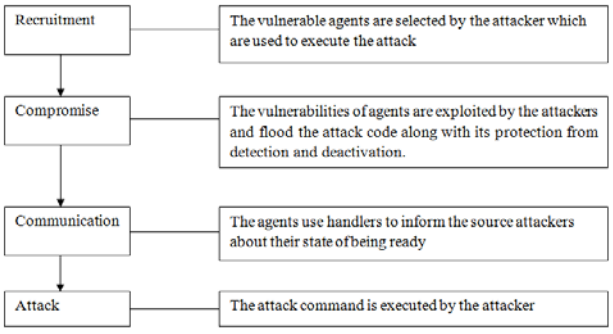

Fig. 2 DDoS description.

Some powerful and advanced tools are available to increase the impact of attack and the potentiality of the attackers to be more ruthless and damageable for the victims e.g. TRINOO, TFN, TFNZK, STACHELDRATH and SHAFT.

3. Related Work

In [21], a framework with security and survivability as major features is proposed by Qian T et.al, as both security and survivability are extremely important for almost all modern wireless sensor network applications. The authors have used composite sensor nodes for single unit architecture of survivability and security. A key management policy is also proposed by the authors along with the major mechanism to manage framework and cooperation between security and survivability together. The results obtained from this mechanism proved that in wireless sensor networks the security and survivability can be improved and enhanced together if a better framework is designed for the system. But in some important scenarios or with some different settings this frame work fails to maintain the balance between security and survivability. This is a major loophole in this framework. To overcome this loophole in this framework (Thein T Chef) [22] proposed another mechanism to deal with the situation when the network failure occurs or there is an attack in the network.

In [23, 24] Boukercheet.al. has explained that the most common and easy targets of the network attacks are localization systems that can damage the entire functionality of wireless sensor network that in turn will spoil military decision making along with other serious issues. In this study they have shown that current localization based system are susceptible to many attacks and how can we use the existing mechanism and methodologies to avoid these harmful attacks in wireless sensor networks. They have divided the security frameworks into distance estimation, localization algo, position competition for secure localization systems. In this research study, the authors have focused and displayed the limitations of localization systems which are currently available. They have also done a thorough study and have mentioned various kinds of attacks on these systems but they have not suggested or proposed any new or updation for an existing mechanism to keep these systems secure. It is difficult to achieve CIA triangle (confidentiality, Integrity, Availability) in wireless sensor networks because of the size of the network and the large number of sensor nodes deployed in different areas and are vulnerable to attacks due to their different constraints. In order to overcome this problem of security and securing the wireless sensor networks from various kinds of cyber attacks, an effective security framework is proposed by Ren et.al.[25] using secret keys which are related to various deployed positions and selected keys are stored on every nodes based on their individual location. This location oriented method binds the effect of compromised nodes effectively to their local hops or local area only without disturbing the security routines. The proposed framework of multi-functional key management and end-to-end data security provides the report of forwarding routes along with node to node and node to sink authentication. The methodology is reliable and efficient in securing the networks from DDoS attacks. The major drawback found in this framework is its complexity and time in efficiency due to its MAC and cryptographic based approach. Another similar framework (Algo) that secures the network form DDoS attacks which is based on localization is mentioned in [24].

In [26] Dsouza et.al. Proposed the secure multipath routing protocol that is based on digital signature and have used a digital signature based on public key to provide authentication between nodes, date integrity but due to the complexity of public key digital signature, they are feasible in wireless sensor networks. In this research article the authors have proposed a cryptographic mechanism to secure the networks from different types of network attacks but they did not provide any technical or practical results. The sensor nodes of wireless sensor networks being computational, power and memory constraints, any method or technique that involves complex competition or requires time is not feasible in securing data or its delivery in the network. D.Pietro et.al. [27] Has proposed a mechanism to deal with above mentioned problems using a deep analysis of security related issues in wireless sensor networks and prepared some techniques to secure the networks from some of the existing attacks in wireless sensor networks. There are many security mechanism that are used to safeguard the wireless sensor networks e.g cryptographic algorithm [28], SKM, security based on MAC [29, 30, 31] etc. and it does not stop here as the research is going on continuously. Every mechanism is efficient and reliable than its previous ones but we have to continue to keep it secure. In this proposed mechanism we used scheme based on IPS which in turn is based on secure routing. We integrated our module with AOMDB protocol and used NS2 (network simulator) to check and analyze the results. The results obtained are impressive and dealing with DDoS attacks in wireless sensor networks.

4. Proposed Mechanism

Algorithm 1

We have designed an algorithm as shown in Figure 3 to scan and analyze the impact of DDoS attack with AOMDV protocol. This attack floods the network with fake packets and consume the bandwidth and the prohibits the legitimate user from sending the genuine data packets.

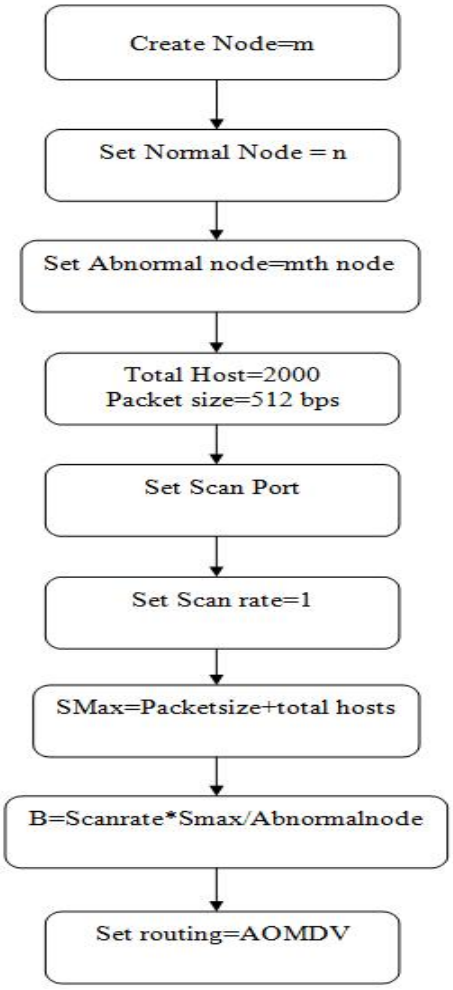

Fig. 3 DDoS Attack

Algorithm 2

Here we present an algorithm as shown in Figure 4 to prevent the DDoS attack using intrusion prevention system. A node P is selected to monitor the behavior of all the existing hops under a specific range and update the routing table about the odd behavior in the network. After this P checks all the data and if it finds any malicious node it blocks the node and sends this information to the sender and the genuine sender node uses another safe route for its data packets.

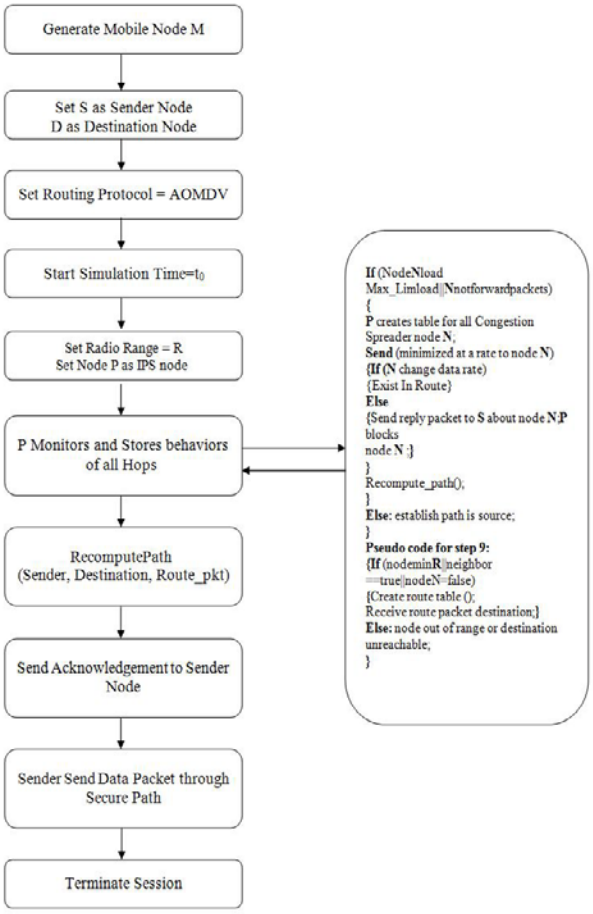

Fig. 4 Proposed Prevention System

5. Simulation and Results

For simulation we used NS-2 to implement AOMDV with DDoS environment and its preventive measures. The parameters used in this simulation and analysis are shown in the Table 1 and Table 2 contains the performance parameters that are used to compare the existing normal protocol's performance with proposed mechanism.

Table 1: Simulation Parameters

Field	Value
Simulator-Version	NS-2
Simulation time	180Seconds
Transmission Range1	120m
No. of Nodes	10-180
Area	800mx800m
Protocol	AOMDV
Transmission Range 2	250m
Speed	0-25 m/s.
App. Traffic	CBR
Packet Size	512B
Traffic Size	5p/Sec
Network Model	R-W Point Model
Pause Time	10,20,40,60,80,100 to 160Seconds
MAC	802.15.4

Table 2: Performance Parameters

Packet Delivery Ratio
Packet Loss %age
Normalized Routing Load
Average and End-to-End Delay

We used 180 nodes to deploy the wireless sensor network for simulating the normal behavior and examine the results using the parameters mentioned in the Table 2. After storing the results, we launched a DDoS attack in the same scenario and deployed our proposed mechanism by selecting a random node as intruder node which generates packet flood and forwards them towards the target and prevents the target from serving the legitimate nodes. It also infects other nodes of the network using the same method. When this attack module was implemented in the normal scenario, the unwanted and malicious packet flood on compromising nodes degraded all the performance parameters tremendously.

In our proposed mechanism, we prepared a secure module, a prevention algorithm that is implemented with compromised network to protect the wireless sensor network from DDoS attacks. Some nodes are elected and set as IPS nodes (Intrusion prevention system nodes) in this methodology and their main job is to scan the network periodically with a selected threshold time within its range in order to find the infected and intruder nodes which generate frequent, large and unwanted packets passing through a specific node. If any such node is detected by the IPS node then all the activities from this node are blocked in the network and this message is send to all the other legitimate nodes in the network which are trying to route their data through this infected node.

In the initial steps we simulated and compared the performance of all the three selected scenarios which included N-AOMDV, A-AOMDV and S-AOMDV by comparing different pause time with all the selected performance parameters including packet delivery fraction, normalized routing load, End-to-End delay and Packet Loss Percentage. The results obtained from this simulation are showed in Figure 5, Figure 6, Figure 7 and Figure 8 respectively. These results proved that all the performance indicators were degraded in A-AOMDV (DDoS-AOMDV) as this specific scenario was having DDoS attack in the network. The pause time increased the performance as the pause time and sensor node mobility are inversely proportional to each other i.e. increase in the pause time will decrease the mobility of the sensor nodes. The results showed that performance using the secure-AOMDV increases tremendously that too approximately to Normal –AOMDV.

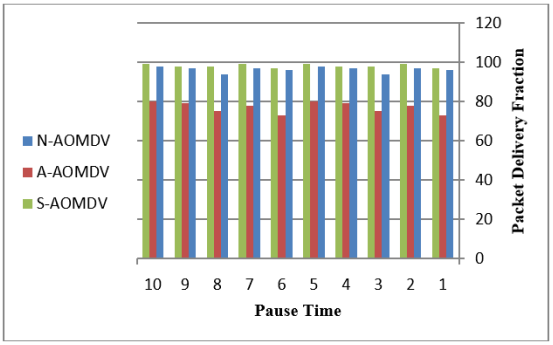

Fig. 5 Pause Time/PDF

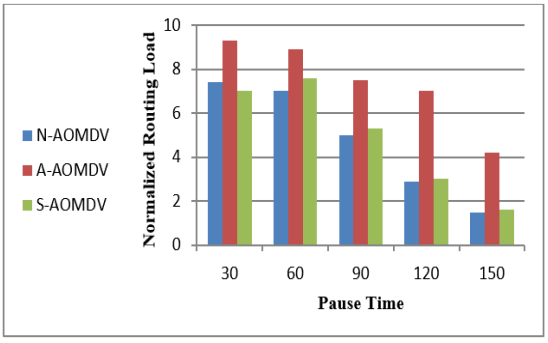

Fig. 6 Pause Time/Normalized Routing Load

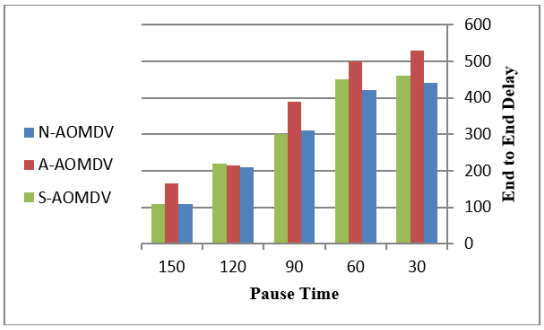

Fig. 7 Pause Time/End-to-End Delay

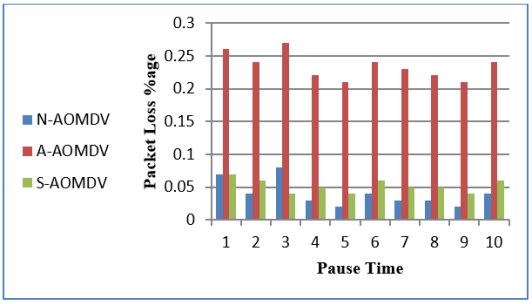

Fig. 8 Pause Time/Packet Loss %age

After this session, we compared all the selected performance indicators with the number of nodes as shown in Figure 9, Figure 10, Figure 11 and Figure 12.

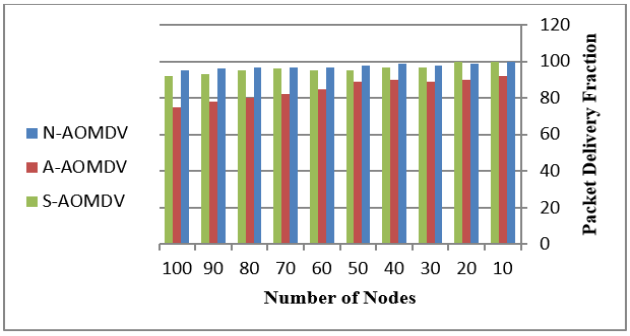

Fig. 9 No. of Nodes/PDF

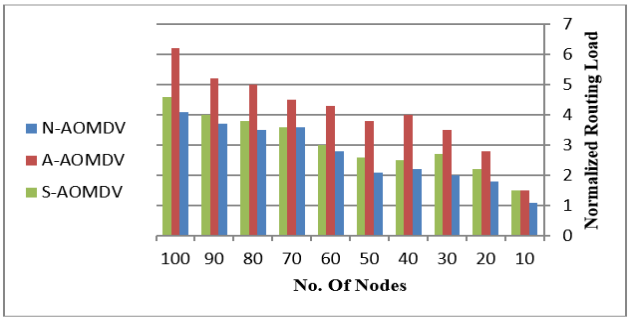

Fig. 10 No. of Nodes/ Normalized Routing Load

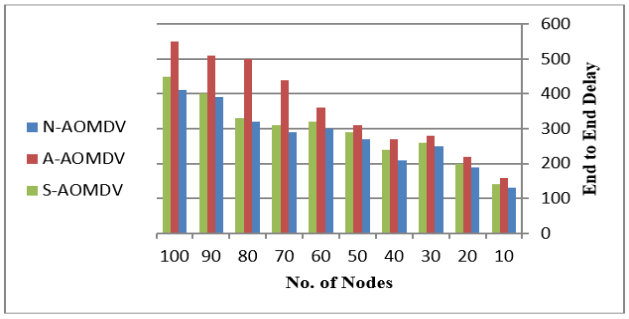

Fig. 11 No. of Nodes/End-to-End Delay

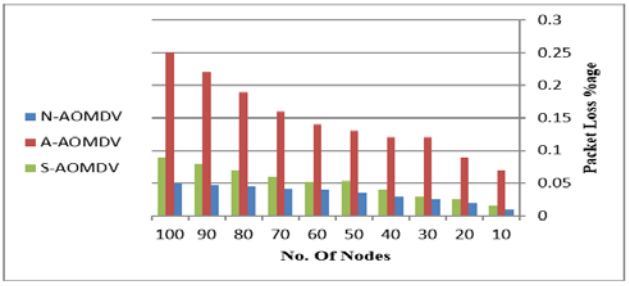

Fig. 12 No. of Nodes /Packet Loss %age

The results show that increase in the number of nodes decreases the performance. Increasing number of nodes means increasing connections for DDoS-AOMDV, thus increasing malicious nodes. The results proved that even in the case of increasing number of nodes, the performance increases almost to that of normal AOMDV using our secure –AOMDV.

6. Conclusion

In this research article, we have proposed an efficient and effective security mechanism against distributed denial of service attacks for wireless sensor networks to maintain the real web semantics of modern world's internet. After simulation, we did a comparative study of parameters to compare the results obtained from our proposed mechanism with normal vector and DDoS vector. Our proposed model is compatible with AODMV and works properly and blocks the infected node that generates the DDoS flood packets in the wireless sensor networks. The results proved a better performance than normal scenario. By applying our proposed mechanism, the performance of the routing protocol is highly improved in presence of a DDoS attack.

Acknowledgement

This research was funded and conducted at Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia during the academic year 2017-2018.

References

[1] Han, G., Jiang, J., Zhang, C., Duong, T.Q., Guizani, M. and Karagiannidis, G.K., 2016. A survey on mobile anchor node assisted localization in wireless sensor networks. IEEE Communications Surveys & Tutorials, 18(3), pp.2220-2243.

[2] Osseiran, A., Boccardi, F., Braun, V., Kusume, K., Marsch, P., Maternia, M., Queseth, O., Schellmann, M., Schotten, H., Taoka, H. and Tullberg, H., 2014. Scenarios for 5G mobile and wireless communications: the vision of the METIS project. IEEE Communications Magazine, 52(5), pp.26-35.

[3] Han, G., Jiang, J., Zhang, C., Duong, T.Q., Guizani, M. and Karagiannidis, G.K., 2016. A survey on mobile anchor node assisted localization in wireless sensor networks. IEEE Communications Surveys & Tutorials, 18(3), pp.2220-2243.

[4] Lu, C., Saifullah, A., Li, B., Sha, M., Gonzalez, H., Gunatilaka, D., Wu, C., Nie, L. and Chen, Y., 2016. Real-time wireless sensor-actuator networks for industrial cyber-physical systems. Proceedings of the IEEE, 104(5), pp.1013-1024.

[5] Dong, M., Ota, K. and Liu, A., 2016. RMER: Reliable and energy-efficient data collection for large-scale wireless sensor networks. IEEE Internet of Things Journal, 3(4), pp.511-519.

[6] Shaikh, F.K. and Zeadally, S., 2016. Energy harvesting in wireless sensor networks: A comprehensive review.

Renewable and Sustainable Energy Reviews, 55, pp.1041-1054.

[7] Fafoutis, X., Vuckovic, D., Di Mauro, A., Dragoni, N. and Madsen, J., 2012, February. Energy-harvesting wireless sensor networks. In Proc. of the 9th European Conf. on Wireless Sensor Networks (EWSN). Trento: University of Trento (pp. 84-85).

[8] Alippi, C. and Galperti, C., 2008. An adaptive system for optimal solar energy harvesting in wireless sensor network nodes. IEEE Transactions on Circuits and Systems I: Regular Papers, 55(6), pp.1742-1750.

[9] Jan, M., Nanda, P., Usman, M. and He, X., 2017. PAWN: a payload-based mutual authentication scheme for wireless sensor networks. Concurrency and Computation: Practice and Experience, 29(17).

[10] Mittal, V., Gupta, S. and Choudhury, T., 2018. Comparative Analysis of Authentication and Access Control Protocols Against Malicious Attacks in Wireless Sensor Networks. In Smart Computing and Informatics (pp. 255-262). Springer, Singapore.

[11] Kumar, R. and Shanmugam, A., 2017. Energy Efficient and Trust Based Black Hole Attack Identification Model in Wireless Sensor Networks. Journal of Network Security Computer Networks, 2(1, 2, 3).

[12] He, D., Chan, S. and Guizani, M., 2017. Cyber Security Analysis and Protection of Wireless Sensor Networks for Smart Grid Monitoring. IEEE Wireless Communications, 24(6), pp.98-103.

[13] Pritchard, S.W., Hancke, G.P. and Abu-Mahfouz, A.M., 2017, July. Security in Software-Defined Wireless Sensor Networks: Threats, Challenges and Potential Solutions. In IEEE Int. Conf. of Ind. Informat., Emden, Germany.

[14] Abdullah Aljumah, Tariq Ahamad,"A Novel Approach for Detecting DDoS using Artificial Neural Networks". International Journal of Computer Science and Network Security, 132 VOL.16 No.12, December 2016.

[15] Abdullah Aljumah, Tariq Ahamad,"Futuristic Method to Detect and Prevent Blackhole Attack in Wireless Sensor Networks", International Journal of Computer Science and Network Security,VOL.17 No.2, February 2017

[16] Tariq Ahamed Ahanger," An Effective Approach of Detecting DDoSUsing Artificial Neural Networks", IEEE international Conference on Wireless Communications, Signal Processing and Networking March 2017

[17] Tariq Ahamad, Abdullah Aljumah," Detection and Defense against Distributed Denial of Service Attack Using Packet Filtration in Wireless Sensor Networks", International Journal of Computer Networks and Communications Security, Volume 5, Issue 12, December 2017

[18] Abdulaziz Aldaej and Tariq Ahamad, “AAODV (Aggrandized Ad Hoc on Demand Vector): A Detection and Prevention Technique for Manets” International Journal of Advanced Computer Science and Applications(IJACSA), 7(10), October 2016.

[19] Luh, R., Marschalek, S., Kaiser, M., Janicke, H. and Schrittwieser, S., 2017. Semantics-aware detection of targeted attacks: a survey. Journal of Computer Virology and Hacking Techniques, 13(1), pp.47-85.

[20] Somani, G., Gaur, M.S., Sanghi, D., Conti, M. and Buyya, R., 2017. DDoS attacks in cloud computing: Issues, taxonomy, and future directions. Computer Communications, 107, pp.30-48.

[21] Y. Qian, K. Lu, D. Tipper, "A design for secure and survivable wireless sensor networks", Wireless Communications IEEE, vol. 14, no. 5, pp. 30-37, 2007.

[22] T. Thein, S. M. Lee, J. S. Park, "Improved method for secure and survivable wireless sensor networks", proceedings Computer Modelling and Simulation UKSIM'09. 11th IEEE International Conference on Sens or Networks, pp. 605-610, 2009.

[23] A. Boukerche, H. Oliveira, E. F. Nakamura, A. A. Loureiro, "Secure localization algorithms for wireless sensor networks", Communications Magazine IEEE, vol. 46, no. 4, pp. 96-101, 2008.

[24] O. Demir, B. Khan, "Finding ddos attack sources: Searchlight localization algorithm for network tomography", 7thIEEE International on IWCMC WirelessCommunication, pp. 418-423, 2011.

[25] K. Ren, W. Lou, Y. Zhang, "Leds: Providing location-aware end-to-end data security in wireless sensor networks", Mobile Computing IEEE transactions on, vol. 7, no. 5, pp. 585-598, 2008.

[26] R. D'Souza, G. Varaprasad et al., "Digital signature-based secure node disjoint multipath routing protocol for wireless sensor networks", Sensors Journal IEEE, vol. 12, no. 10, pp. 2941-2949, 2012.

[27] R. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, G. Tsudik, "Data security in unattended wireless sensor networks", Computers IEEE Transactions on, vol. 58, no. 11, pp. 1500-1511, 2009.

[28] M. H. Eldefrawy, M. K. Khan, K. Alghathbar, "A key agreement algorithm with rekeying for wireless sensor networks using public key cryptography", IEEE International Conference on Wireless Sensor Networks, pp. 1-6, 2010.

[29] K. V. Arya, S. S. Rajput, "Securing AODV routing protocol in MANET using NMAC with HBKS Technique", IEEE International Conference on SPIN, pp. 281-285, Feb 2014.

[30] R. D'Souza, G. Varaprasad et al., "Digital signature-based secure node disjoint multipath routing protocol for wireless sensor networks", Sensors Journal IEEE, vol. 12, no. 10, pp. 2941-2949, 2012.

[31] M. Das, "Two-factor user authentication in wireless sensor networks", Wireless Communications IEEE Transactions on, vol. 8, no. 3, pp. 1086-1090, 2009.