Journal of trends in Computer Science and Smart technology (TCSST) (2020)
Vol.02/ No. 03
Pages: 134-140
https://www.irojournals.com/tcsst/
DOI: https://doi.org/10.36548/jtcsst.2020.3.002

A Novel Hybrid Routing Algorithm with Two Fish Approach in Wireless Sensor Networks

Dr. N. Bhalaji,
Associate Professor,
Department of Information Technology,
SSN College of Engineering,
Old Mahabalipuram Rd, Kalavakkam.
Chennai, India.
Email id: bhalajin@ssn.edu.in

Abstract: Over the years, Internet of Things has advanced greatly advanced with technological inventions, enabling the development of smart networks globally. Network edge is introduced into the architectures in order to provide better user experience and quality of service But the issue with this these systems should be able to resist the attacks from external sources. There are many existing methods which are concerned with detecting the intrusion over static wireless sensor web. Due to various transmission regions being involved when using the sensor nodes, it is challenging task to choose the right guard nodes and sensor monitoring nodes. In order to address this issue, we propose a safe monitoring and routing protocol that incorporates Artificial intelligence on the basis of Authentication and Encryption Model. Analysis of the proposed work shows that it proves to be more efficient when compared to other routing and monitoring methods.

Keywords: Artificial Intelligence; Smart Network; Internet of Things; Secure Routing and Monitoring; Guard Nodes;

1. Introduction

One of the recent development as the result of III Industrial revolution is the transmission of data over the internet by interfacing devices with the Internet, giving them the ability to be controlled using packets of data [1]. Initiated in the year 2006, the number of devices in which IoT has been incorporated has increased to over 200 billion. IoT intervention in transportation, healthcare, energy, finance, education and smart cities has led to a smarter environment [2]. As a result of this, industry, academia and individuals have worked hard to provide safety and security for these networks and devices [3]. The catastrophe condition of the security of the system will be exposed to the botnet and hackers who are looking to hack into the system [4]. Similarly cooperating an individual channel will make the system powerless. Botnets as connective devices were gathered in Dyn cyberattack in 2016. With progress in technology, there have been advancement in the complexity and diversity of the attack vectors [5]. Hence Wireless Sensor Networks (WSN) has become essential to gather information about the nodes, calculate the output into data and to transfer the gathered information to the receiver. Any sensor can be used, based on the data to be observed such as magnitude, pressure, temperature, flow and level sensors etc [6]. Since the use of wireless medium will make the device defenceless and weak, it will be difficult to secure the data from attackers and hackers when compared to other networks which are more sturdy and wired [7].

Wireless Sensor Nodes are used in defence-oriented devices and in battlefields which can be used to identify biological or chemical vapours, electromagnetic signals, lights, border violations and presence of strangers or enemies [8]. Enabling a sturdy security in such an optimized WSN is a difficult task as protecting the nodes will require changing the adversaries as well as coordinating the sensor nodes' location [9]. Many cases of attacks have been observed over the past few years based on the objectives. In fact, it is possible for sufficient software and hardware to behave as an adversity and misinterpret the data in an unethical manner. These adversities might also cause the sensor nodes to manipulate the activities of the wireless sensor network such that it will decrease

ISSN: 2582-4104
Submitted: 27.05.2020
Accepted: 09.07.2020
Published: 17.07.2020

the service, throughput and performance of the sensor nodes. An intrusion Detection System is used to detect and take measures to prevent these vulnerability attacks and activities [10-11]. It can be used in wired network along with the hardware system required to observe the activities of the network.

The proposed methodology provides an appropriate solution to address the network intrusion with the help of a secure monitoring and routing algorithm [12]. The contributions of this paper are as follows:

- A hybrid routing scheme which incorporates the protocol for routing the data.
- The proposed routing and monitoring mechanism can behave as a reactive and proactive device using the novel two-fish approach
- To choose the best path to transmit the information based on using optimized algorithms that can help in securing the transmission.
- Based on sensor network energy levels, network functionality, consecutive update rate, frequent link breaks, nodes mobility and network scenario, the optimal routing path is determined.
- They are further trained to be incorporated using artificial neural network.

In general, the best path to reach the destination can be determined using the routing protocol. However, it does not decide on the right nodes for monitoring [13]. Hence the monitoring and routing algorithm is proposed in order to secure better transmission over many channels.

2. Proposed Architecture

The proposed methodology is represented in the given architecture shown in Fig.1. Here the data observed in real time are recorded and are transmitted into a collection of bits which can be sent to the neighbouring nodes. In the Wireless Sensor Nodes, one or many senders may be used transfer information to the desired destination. However in a WSN, there are multiple reactive and proactive protocols which can be used to choose the right path in which the packets should travel. This protocol is programmed to be compatible to train in artificial neural network. This type of protocol will not be efficient in terms of security scalabilities, error identification, route discovery and throughput. The reactive protocol will be used in acquiring minimum overhead. However, it will not effective for dense networks and might cause delay in determining the right route. On the other hand, the use of proactive protocol will be efficient in finding the route and further, it is always updated and is the apt choice for networks that are of large size. Hence a hybrid routing protocol is proposed in this paper which makes use of the optimum functions of other routing protocols. The proposed work uses routing that is implemented with multipath fashion.

ISSN: 2582-4104
Submitted: 27.05.2020
Accepted: 09.07.2020
Published: 17.07.2020

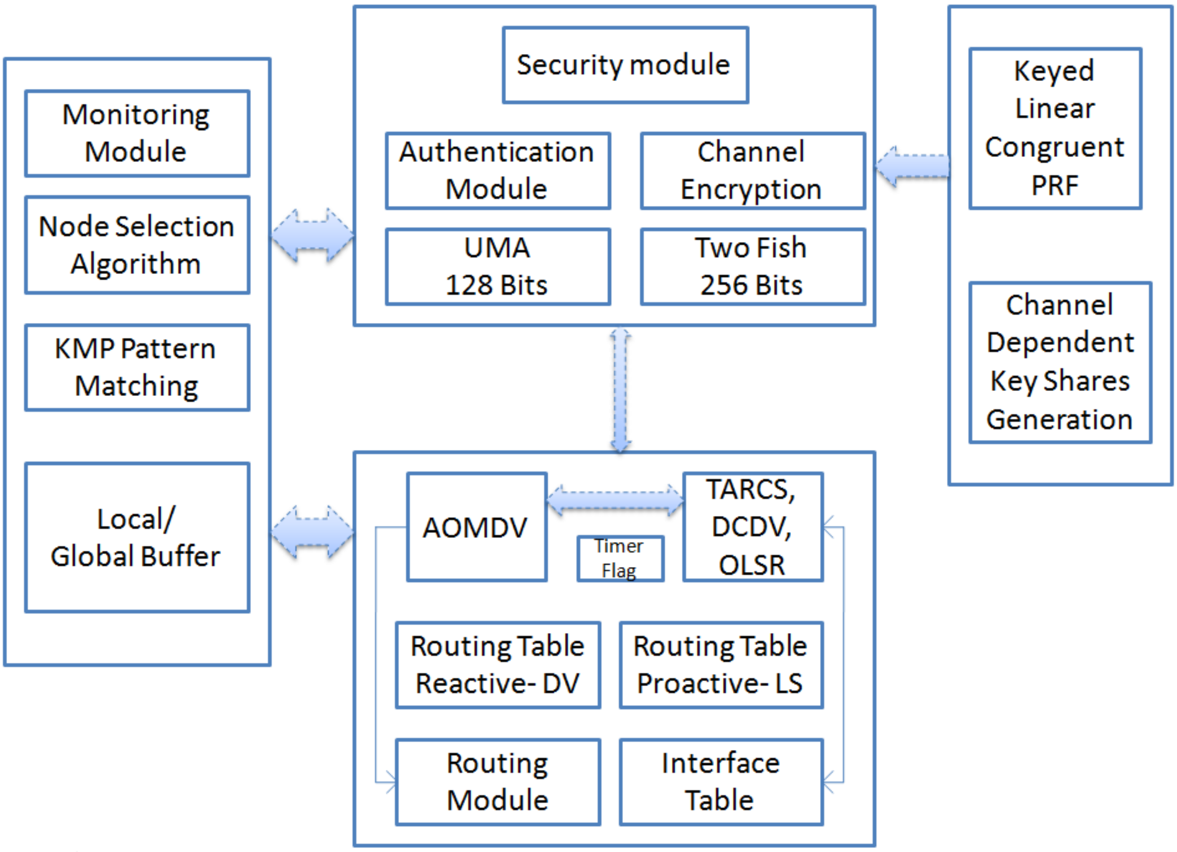

Fig.1. Architecture of the Proposed Methodology

3. Algorithms

3.1 Initial Selection Phase

The monitor nodes will be selected using the initial selection phase algorithm where both the path and neighbours are identified individually using a route that is less redundant in nature by in the presence of the link. Initial Request is sent at different intervals of time as INITREQ to the neighbouring nodes. The node then waits for the response of Initial Response as INITRES from the node which receives the request. There might also be many destinations and sources for the sensor network. This method is incorporated to observe the nodes in a safe manner in order to analyze adversary as well as network traffic. Using this algorithm, multiple path approach is used which cannot be unavoidable.

ISSN: 2582-4104
Submitted: 27.05.2020
Accepted: 09.07.2020
Published: 17.07.2020

3.2Multi-Point Relays Algorithm for Initial Setup and Neighbour Identification

In this algorithm, the request for initial request is broadcasted. On noticing the broadcast, the source which receives the broadcast will initiate connection in the form of hello packet. This can then be used to identify the neighbouring nodes and based on Optimised Link State Routing (OLSR) approach, a request is sent. Before MRP algorithm is initiated, the neighbours and the links are joined together in order to identify the link codes. Based on minimal redundant responses and requests, hops with the neighbours are set. Moreover, this algorithm will also be used to update OLSR by means of checking the responses and requests in the form of a sequence. The initial selection phase will be determined by the algorithm proposed in section 3.1 which is used to monitor the nodes. Initial Request is sent at different intervals of time as INITREQ to the neighbouring nodes. The node then waits for the response of Initial Response as INITRES from the node which receives the request.

3.3Multiple Channel Selection

When to Concealed Monitor sets are built by the OLSR, it will trigger the timer to go off, alerting the Ad Hoc On-Demand Multipath Distance Vector (AOMDV) to comply with monitoring the data as and when essential. In order to obtain the information about the neighbours and the nodes, a Protocol Interface Table is used. Similarly, this can also be used to develop the routing path to monitor the data which will be called the Sandwich Routing Table that is sustained using AOMDV. This algorithm will also demand maintenance of different channels and monitoring of the routes as and when in demand. Hash-based Message Authentication Code is used for ensuring authenticity of the data amidst traffic pattern under observation by the chosen sensor node. Finally channel-dependent key shares will be used to encrypt the data in the proposed novel Two fish algorithm.

3.4 Key Shared Dependent on Channel

Using Keyed Linear Congruent Pseudo-Random Function, we aim to build the absolute random key.

$$P_c = \{PSQN \parallel T_N \parallel AT_P \parallel TT_L \parallel DT_N \parallel T_{MID} \parallel T_{MSG} \parallel T_{MPR}$$

where T_{MSG} is the Timestamp of message validity, T_{MID} is the timer of message, DT_N is the Dupe Timer of Nodes, TT_L is the Tuple Time, AT_P is the Association Timer of pairs, T_N is the Node's Timer, T_{MPR} is the MRP Timer and PSQN is the Packet Sequence Number. An absolute random key is essential in order to choose the right node tuple. A set of nodes are chosen in a random fashion, represented by P_CFrom the tuples, a set of multi-variants were chosen such that they can be used to develop channel-dependent variable key shares. These keys are encrypted with 256/192/128 bits of encryption block which will be used to properly determine the level of security that is provided for other applications in which it is incorporated.

3.5 Secure Transmission and Route Maintenance

When formation of Concealed Monitor Set (CMS) is completed by OLSR, it will result in triggering the timer. This will further enable AOMDV to incorporate the monitoring strategy required. This algorithm will be used to recover details of neighbours and nodes with the help of a protocol interface table incorporated using OLSR.

AOMDV routing table will continue to develop the routing path. This table is also referred to as the Sandwich Routing Table.

4. Results and Discussion

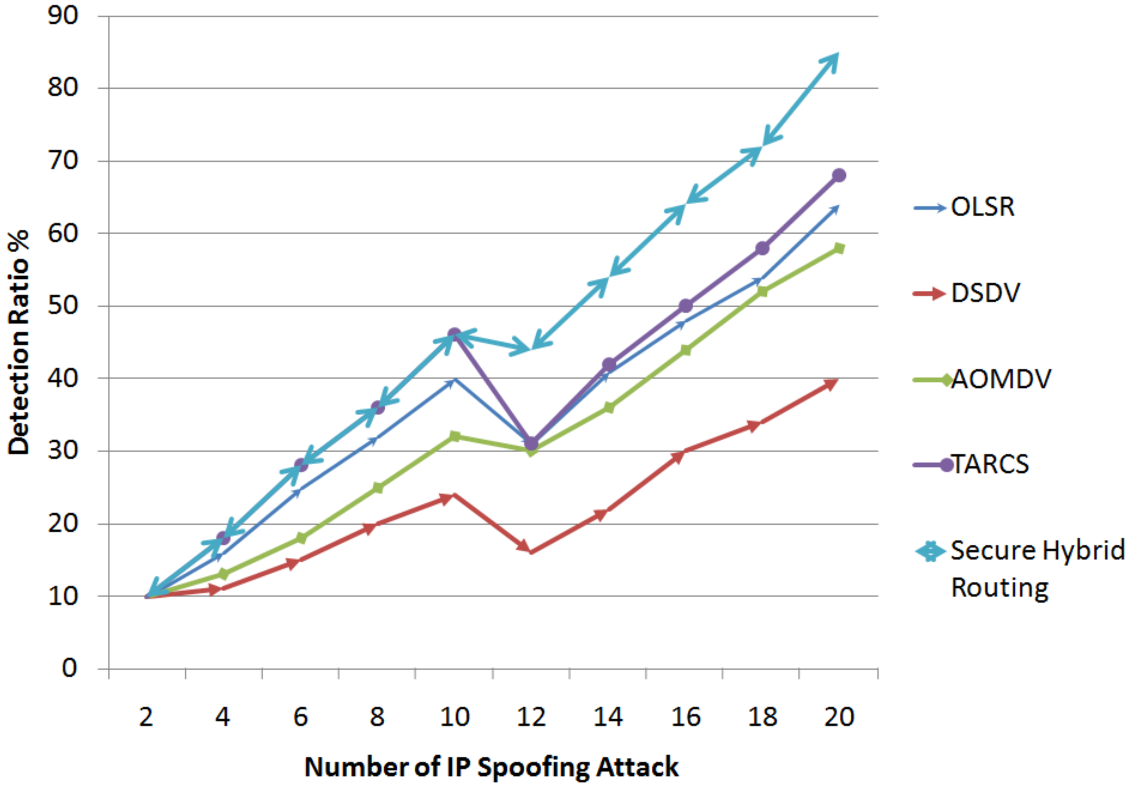

Fig.2. Detection of IP Spoofing Attack

Fig.2 and Fig.3 represent IP spoofing attack and detection ratio for wormhole attacks. In order to intrude or interpret the data transfer, attackers will attempt to compromise the node or channels at the routing and MAC layer. This graph gives an overview of the security level imposed by the different layers to defend against mobile sensor attackers. For the different attacks in network nodes and links, the attack detention ratio is represented in the figures Fig.2 and Fig.3. Moreover, it also shows the results for routing overhead in issues of mobility aspects. The sensor nodes or ideal nodes which use minimal velocity and least amount of transmission rate are determined from their respective paths. This will also affect the overhead of the nodes or the network. The observed experimental results can also be compared with other similar methodologies implemented and it is found that the proposed methodology performs better than the peers.

ISSN: 2582-4104
Submitted: 27.05.2020
Accepted: 09.07.2020
Published: 17.07.2020

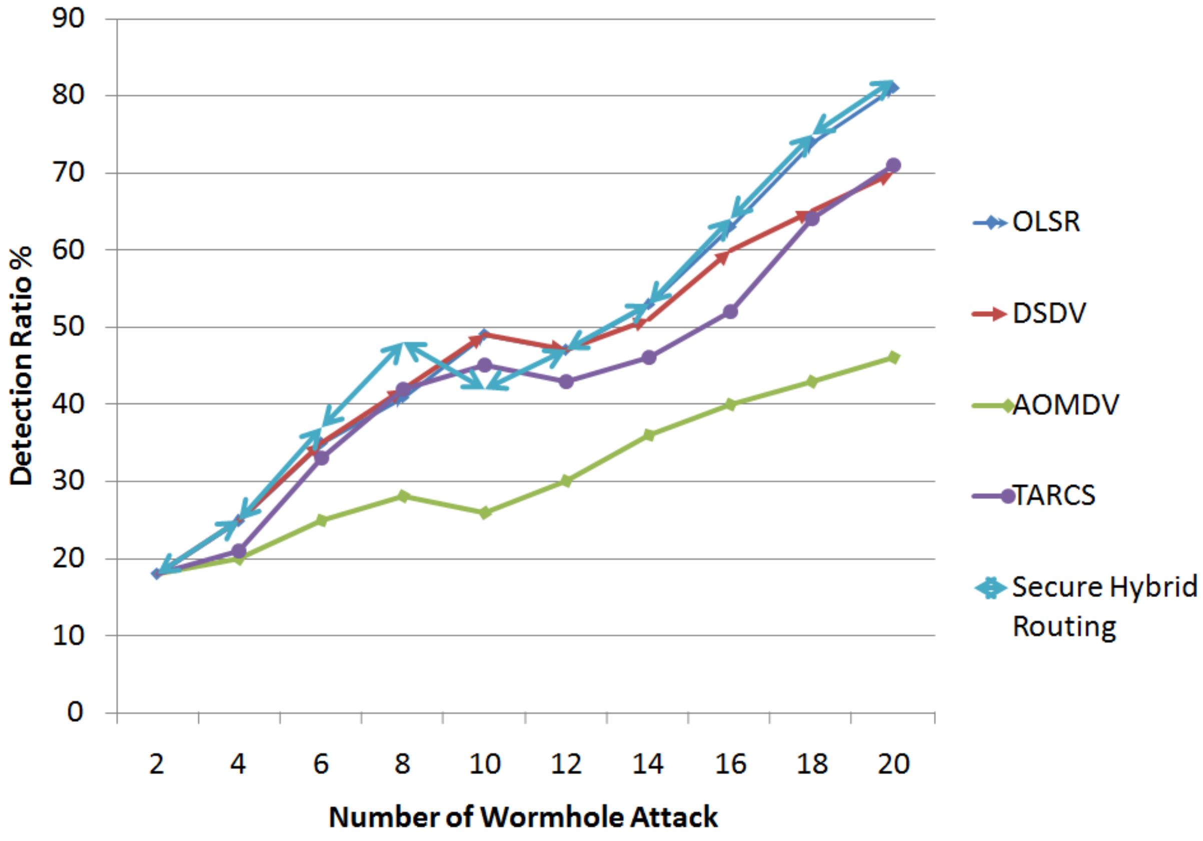

Fig.3. Detection of Wormhole Attacks

5. Conclusion

The proposed methodology of monitoring and routing is implemented such that it can help enhance the security level of the transmitted data and the use of artificial neural network will further enhance it to be adaptable to the network environment. In order to improve security, monitoring and routing protocols using symmetric key approaches are incorporated. This algorithm is proposed based on Eligibility Weight Function and Authentication and Encryption Model which can be used to choose the apt sensor guard nodes using a symmetric key approach. With the help of Serpent, RC6, MARS and Twofish approach as the base, the proposed approach is developed. It is used to select the sensor monitor node which will help improve the security of the system. This will also enhance how securely data can be transmitted with ad hoc sensor network. A completed research on the simulation results show that the proposed methodology is very effective and holds a better rate of detection and monitoring ratio when compared with the other methodologies. The future for the proposed algorithm lies in implementing this mechanism to determine the results of the protocol. It can also be expanded to be used in WSNs for ensuring that the security layers are authentic.

ISSN: 2582-4104
Submitted: 27.05.2020
Accepted: 09.07.2020
Published: 17.07.2020

References

[1] Yu, X., Fan, F., Zhou, L., & Zhang, F. (2016, June). WSN monitoring area partition clustering routing algorithm for energy-balanced. In *2016 6th International Conference on Electronics Information and Emergency Communication (ICEIEC)* (pp. 80-84). IEEE.

[2] Enxing, Z., &Ranran, L. (2017). Routing technology in wireless sensor network based on ant colony optimization algorithm. *Wireless Personal Communications*, *95*(3), 1911-1925.

[3] Elleuchi, M., Boujelben, M., Obeid, A. M., Abid, M., &BenSaleh, M. S. (2016). Power aware deployment and routing scheme for water pipeline monitoring based on Wireless Sensor Networks. *Journal of Information Assurance & Security*, *11*(5).

[4] Bhatti, R., & Kaur, G. (2017, January). Virtual grid based energy efficient mobile sink routing algorithm for WSN. In *2017 11th International Conference on Intelligent Systems and Control (ISCO)* (pp. 30-33). IEEE.

[5] Sathesh, A. (2019). Enhanced Soft Computing Approaches For Intrusion Detection Schemes In Social Media Networks. *Journal of Soft Computing Paradigm (JSCP)*, *1*(2019), 69-79.

[6] Zhang, J., Lin, Z., Tsai, P. W., & Xu, L. (2020). Entropy-driven data aggregation method for energy-efficient wireless sensor networks. *Information Fusion*, *56*, 103-113.

[7] Li, F., Liu, M., & Xu, G. (2019). A quantum ant colony multi-objective routing algorithm in WSN and its application in a manufacturing environment. *Sensors*, *19*(15), 3334.

[8] Varshney, S., Kumar, C., & Swaroop, A. (2018). Leach based hierarchical routing protocol for monitoring of over-ground pipelines using linear wireless sensor networks. Procedia Computer Science, 125, 208-214.

[9] Haoxiang, W., &Smys, S. (2020). Soft Computing Strategies for Optimized Route Selection in Wireless Sensor Network. *Journal of Soft Computing Paradigm (JSCP)*, *2*(01), 1-12.

[10] Guo, P., Liu, X., Cao, J., & Tang, S. (2017). Lossless in-network processing and its routing design in wireless sensor networks. *IEEE Transactions on Wireless Communications*, *16*(10), 6528-6542.

[11] Tan, C., Ji, S., Gui, Z., Shen, J., Fu, D. S., & Wang, J. (2018). An effective data fusion-based routing algorithm with time synchronization support for vehicular wireless sensor networks. *The Journal of Supercomputing*, *74*(3), 1267-1282.

[12] Liping, L. V. (2017). An energy aware multipath routing algorithm for wireless sensor networks. *International Journal of Online and Biomedical Engineering (iJOE)*, *13*(04), 45-56.

[13] Sathesh, A. (2019). Optimized Multi-Objective Routing For Wireless Communication With Load Balancing. *Journal of trends in Computer Science and Smart technology (TCSST)*, *1*(02), 106-120.

ISSN: 2582-4104
Submitted: 27.05.2020
Accepted: 09.07.2020
Published: 17.07.2020