International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2016/v3/i4/48569 Volume 3, Issue 4, July – August (2016)

RESEARCH ARTICLE

A Novel Routing Scheme to Avoid Link Error and Packet Dropping in Wireless Sensor Networks

M. Kavitha
Research Scholar, S.T Hindu College, Nagercoil-2, India.
kavi.mkv77@gmail.com

B. Ramakrishnan
Department of Computer Science and Research Centre, S.T Hindu College, Nagercoil-2, India.
ramsthc@gmail.com

Resul Das
Department of Software Engineering, Firat University, 23119, Elazig, Turkey.
rdas@firat.edu.tr

Abstract – Packet loss is a major issue in Wireless Sensor Network (WSN) data transmission which is caused by malicious packet dropping and link error. In conventional methods, the malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the stochastic processes that characterizes the two phenomena exhibited in different correlation which would affect the network performance i.e. detection accuracy. By detecting the correlations between lost packets, we will decide whether the packet loss is purely due to regular link errors, or is a combined effect of link error and malicious drop. In order to overcome these issues, we have proposed a HLA (Homomorphic Linear Authentication) based on routing protocol which is a collusion proof mechanism and resolves the public auditing problem. Here, the proposed technique will be implemented in OLSR (Optimized Link State Routing) Protocol. The actual status of each packet transmission i.e., the packet loss information can be described by our technique. The network simulation results describe the performance of the proposed method in terms of detection accuracy in low computation complexity. Our HLA based OLSR protocol is compared with existing AODV, RIP and other protocols.

Index Terms – WSN, AODV, OLSR, HLA, malicious node attack, Link Error.

1. INTRODUCTION

Wireless sensor network is a simple and efficient mechanism through which the data can be transmitted from the source to destination. The main use of the WSN is to maintain the security of the data packet while it travels from one hop to another. Hop can be easily misbehaved through the energy wastage. [1] Thus WSN process is a complexity network to transmit the data onto one source to another. Wireless sensor network is mostly constructed with the help of set of nodes. And the process of performing the data transmission is based upon simple and efficient scheme. The nodes are interconnected with the help of links and routers. The main use of the processing ability is to transmit the data from one to another in a single and multi- node.

W. Mao the research scholar expands the Modern theory of cryptography that will increase the security of the passage through which the data can be safely protected in a unique format. This should be further added to the network to transmit the data with integrity constraints. [2] Adi Shamir expresses the idea of threshold scheme that can be very helpful in the cryptographic keys. We can encrypt the data to protect it. Threshold scheme is highly untrustworthy since a single misfortune can make the information inaccessible.

The previous model focuses on reducing the packet dropping attack by implementing several process step activities. The systematic development of the model is used to develop the execution of the auto correlation process. A simple mathematical representation is used in above process. The node activities can be easily changed by performing the simple and efficient process. This should be easily processed by checking the packet dropping framework of the system. A diagrammatic representation of the model is shown below.

Lamport says “A method of user’s password authentication is described as is it secured even if an intruder can read the system's data [3]. This is implemented with a help of microcomputer and it assumes a secure encryption method. Thus more or less every user needs to perform some other performances related activities to protect their own data. [4] Vanstone told that the pass breakers more or less can be used to produce the possible declaration of the system though the concept of simple and elegant format.

As shown in the Figure 1 the data is stored in simple and efficient model. User is responsible to maintain the system and transmit the data from the unsecured network. The packet

RESEARCH ARTICLE

dropping attack is easily solved by the mechanism overcoming by the system representation. The previous RIP and AODV protocol is not useful for processing data in the complex network.

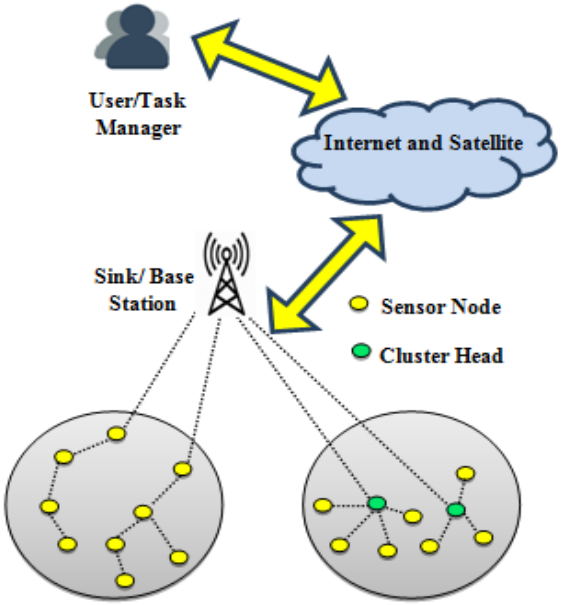


Figure 1 Wireless Sensor Network

A mobile ad hoc network is created by wireless hosts which may be mobiles that are capable of communicating with each other and infrastructure less network. [5] MANET problems are not easy to be solved. The routing security issues of MANETs, and the "black hole" problem-analyze that can easily. [6] The "black hole" is the main problem that affect the security of route that means “node can be received data but it does not send data with its neighbor”. Another problem: “sinkhole problem” that means when user assigns unique information, the node that has presented the information is trustworthy node”. The black hole problem for ad hoc on-demand distance vector routing protocol has been solved by our proposed method. There are two types of networks: a) Flat based network and b) cluster based network. In Flat based network each nodes is interconnected with its neighboring node. But the cluster based network is simple and can be used easily, when comparing with the flat based network. Here the cluster based network is more useful than the flat one system. Thus the node equality is commonly grouped into the system. The proposed model is suitable for both flat based and the cluster based concept.

Another type of network is called as VANET, B.Ramakrishnan et al. describe the time needed to send or received the message in the intelligent transfer system [7]. Describes a novel clustering concept in which this paper purposes a highway vehicular model among the MANET node. B.Ramakrishnan et al [8] propose the main aim of the mobility model is to reproduce some of the features of vehicle in VANET. Mahattan mobility model is being used by many researchers. To move packet among the vehicles, a competent routing protocol is used.

B.Ramakrishnan proposed a cluster based simple highway mobility model with routing AODV. By using the VANET MAC layer the packet receiving and delivery ratio is measured. This paper also describes analyzation of services discovery procedure [9]. M.Milton Joe et al. describe a comprehensive characteristics of vehicular network and also design a new GSM based mobile network communication in vehicular network. It establishes communication between vehicle and mobile phones. It proves its efficiency by the metrics of the GSM based mobile network communication [10].

2. RELATED WORKS

Because of the importance of wireless sensor networks, many academic works have been done to improve the performance of networks. In the meantime, there are a lot of related papers about this subject.

Tao Shuand Marwant Krunz proposed and elaborated the idea about Mobile Data Off-loading in an offload infrastructure. Users forward the packets using hand held devices through access points. Each data packet reaching the destination correctly is one of the challenging tasks. Customers willing to forward the data packets across the network, may depend on the others or traffic occurred. This model proposes how the data packets successfully reach the destination with “tightness” concept. This system promotes to reduce the network resource utilization and cooperative behavior among other nodes [11].

Awerbuch et al. [12] proposed airborne network is an evolving field in the wireless networks. Airborne network is an efficient routing protocol and it is suitable for larger size network. It is based on performance, routing model, network structure and methodology. Performance of routing protocol is tested by a simulator. Performance like packet delivery ratio and time is varied due to other nodes. These parameters are considered for evaluating routing protocol. Method used in the AeroRP, similar to the discovery of neighbors is varied for different protocol [12].

Balakrishnan et al. [13] proposed routing protocol in mobile ad-hoc networks. Collection of nodes is called as network which are connected dynamically without using any infrastructure. Various types of routing protocols have been implemented such as OLSR, DSR, YMO, AODV, DSDV, BATMAN etc. The comparison is based on relative DYMO, OLSR and DSR protocols.These protocols are implemented in a different simulation environment. The proposed work has been selecting a suitable routing protocol. These three protocols are simulated in a sample network using set of parameters [13].

RESEARCH ARTICLE

Gerhards et al. [14] proposed a mobile ad hoc network (MANET) which has no centralized administration. In MANET, the collection of mobile ad hoc node acts as self-organized nodes with dynamic topology. It has no pre-existing infrastructure. MANET nodes act like both host and the router. It transfers the data using multi-hop ways to each other by forwarding packets. The fundamental characteristics are open medium and dynamic network topology and the management is deficient in network are particularly affected by various type of attacks. Many other secure and robust routing protocols have been designed and many security schemes have been recommended to tackle these issues in the security. In MANET, routing attacks are particularly severe due to presence of malicious nodes [14].

Das et al. introduced the layers of OSI model are targeted by many security issue [15]. There are different types of attacks such as Distributed Denial of service, Man-In-Middle and IP Spoofing attack. This paper tries to overcome these attacks.

W. Yu, Y. Sun and K. R. Liu proposed how to prevent the vampire attacks in many popular protocols [16]. This model provides methods to reduce the attack in a Cluster Head. Cluster Head employs in vampire attack and transmits the packet without dropping. It gives a successful and reliable message delivery even in case of Vampire attack. In worst case, Network-wide energy is increased by single Vampire usage.

The previous paper mentioned is not simple and cost effective. To overcome this model, the data processing is substitute with simple and efficient way through which it can be designed and performed for a previous day process in an elegant way. Thus the proposed model is implemented to design a perfect format for performing a simple transaction processing for the system. The different way of processing issues can be maintained by the network as a simple and efficient way for processing the input.

Ramakrishnan et al. proposed a design of adaptive routing protocol based on cuckoo search algorithm [17]. This protocol combines topology and geography routing protocol and provides the secure transmission. To find the route this algorithm uses a local stochastic broadcasting.

A.Anuba Merlyn and A.Anuja Merlyn proposed an energy efficient routing approach and a new algorithm called descriptive delay function.[18]. In that algorithm RTS/CTS message handshaking mechanisms is used for data forwarding.

Baykara and Das proposed honeypot system combined with IDS/IPS. Honeypots are used to analyses real time malicious attack. This system reduces the falls positive alarm level. IDS combined with honeypot are used to detect new attack [19].

R.S Shaji et al. described a routing scheme called SFUSP used for finding the best path in heterogeneous environments. This scheme works with efficient broadcasting technique cluster based message and passing method are used to find the weaker nodes [20].

Namesh and Ramakrishnan proposed a vector based forwarding routing protocol in two different architectures. They are static nodes and moving nodes. The VBF is a highly recommended protocol, which consumes low energy, high throughput, high packet delivery ratio and low packet dropping ratio [21].

Bhagavanth et al. describe an improved hybrid signcryption method which is based on KEM and DEM algorithm. In signcryption algorithm, ECC method is used to create a private and public key. It has certain advantages such as high security, high speed and low bandwidth [22].

Karadogan and Das describes the packet was transmitted with header information, Header information contains details about the destination address and the route, if the header information is corrupted the packet unable to reach the destination. This paper describes how this drawback can be overcome by using different technique [23].

3. PROBLEM IDENTIFICATION

In existing model for maintaining a simple processing capability, the data can be securely transmitted from one side to another. The basic data transmission is simple but the security is still lacking. The existing model is only supported to find the untrustworthy node/hop in the network. The contribution of the system is to find the malicious node in a simple and efficient way. Thus the data can be easily send to one process to another. The main use of the previous mechanism should be formatted under different scenarios.

The main aim of processing is to detect the malicious node. The processing of maintenance is to follow the basic maintenances that are provided. The system is maintained to form the systematic representation. The formation of the model is to be maintain under the scheme through which it can be formed. The systematic development of the process can be used under different sources of mechanism through which it should be solved.

3.1. High Malicious Dropping Rates

The data which fails to reach the destination is described as packet loss. Most (All) the packet loss are caused by malicious dropping. Most networks may be have failed by packet dropping. This method is used to identify the malicious nodes.

3.2. Credit Systems

A credit system provides a motivation for responsiveness. All the nodes are relied by other nodes. Each node receives credit and is used to send their packets.

RESEARCH ARTICLE

3.3. Authority Systems

The authority of the system depends on other nodes to monitor and find untrusted neighboring nodes. High packet dropping nodes are getting a bad authority by the neighboring nodes. This information is periodically updated and the entire network is used to create a strong route. This may help to remove malicious nodes in the network path.

3.4. End to End Acknowledgements

When packet loss occurs, it directly locates the hops. A node with highest packet loss rate in the route can be rejected. These are some of the process for avoiding serious threats. These are to be maintained by following different source of parameter.

3.5. Cryptographic Methods

Forwarding packet at each node constructs proof by the bloom filters. Relayed packets are investigated at successive hops in the network path that helps to find doubtful hops.

3.6. Malicious Dropped Packet vs. Link Error

The number of packet dropping is higher than the reason by link errors, but the consequence of link errors is unavoidable.

3.7. Architecture of Problem Identification

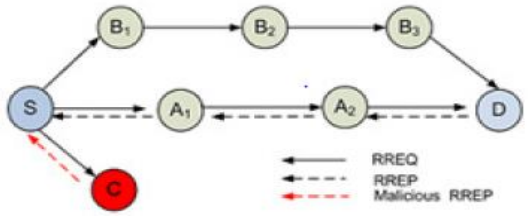


Figure. 2. Architecture of Problem Identification

In above Figure 2, C is a malicious node intending to drop packets from S to D. To discover a path from S to D, S first broadcasts RREQ packet to its nearest one. For each nearest node continues to rebroadcast this message as explained earlier, until it reaches D. The malicious node C ignores this rule and lies to S claiming it has the shortest path to D and sends a RREP packet to S. Now, S assumes that the shortest route to D is through C and starts to send data packets to D through C which is in turn dropped.

$$fc(i) = E \{ aj\ aj+1 \} \text{ for } I = 0, \ldots\ldots\ldots\ldots M$$

At different time, ARR representing the packet transmitted is received by the destination or lost before reaching the destination. There is an auditor in the routing path of the nodes. Auditor doesn't have any knowledge about the nodes. Auditor is used to detect the malicious node when it receives ARR request from the source. Feedback is received from source to destination. The integrity and authenticity of D is verified by elliptic curve digital signature algorithm. ARR sends a conformation request to all the nodes and waits for their ACK and if any node doesn't send an ACK to ARR that node is noted as malicious node. The attacker's aim is for discarding or dropping the packet to reduce the network performance. Malicious packet discarding can be any type (i.e.) it may be a significant packet or random packet. There are some of the collisions between malicious nodes. So, a malicious node establishes separate routing path apart from the original routing path and transmits its packet to the malicious node in which this form of exchange can't be detected by the auditor

3.8. Drawback

The main drawback found in the existing model is the Link error finding. This drawback is overcome by the proposed model. A scheme called elegant routing is used to overcome the computation and communication overhead in the network.

4. PROPOSED MODELING

In this research work the existing drawback is to overcome by finding the Link Error. This can be done by the implementing the robust routing scheme that is better than the existing AODV protocol. The protocol modification is done by replacing AODV with OLSR routing work. Another use of the proposed work is used to maintain truthful detection by implementing HLA. Thus the packet dropping detection is simple. But the link or route implementation is based on the OLSR routing concept. The OLSR is abbreviated as the Optimized Link State Routing scheme. These schemes are simple and cost effective through the proposed model. Additionally, anchor node is implemented to maintain the route details and the node details in that the node guides the data to transmitting along the trustworthy node. Thus the implementation requires less cost and time to maintain a routing scheme in the network.

The security algorithm used in the research work is the Ceaser cipher cryptographic Algorithm. This algorithm is simple and robust to overcome the packet dropping attack in the network. Thus, this should be used to maintain under the simple and efficient scheme. As shown in the figure the data that is used to maintain a simple and efficient algorithm for which it can be used for different purposes.

4.1. Proposed Architecture Modeling

The main use of the research work shown in the Figure 3. To simplify the systematic update of the meaningful environment through which it can be used. The HLA mechanism is introduced to process the simple and the OLSR routing protocol. The purpose of HLA is to send a "HELLO" message to all nodes and wait for the ACK from all nodes. Only some nodes are send an ACK to HLA, and these nodes are identified as trustworthy. Now the nodes can transfer the packets by finding the shortest path in the trustworthy node list. Another use of HLA is to monitor all the nodes, if the destination nodes don't receive the packet, it sends an ACK to HLA. Now HLA

RESEARCH ARTICLE

starts monitoring and finds the malicious node which holds the packet or if any link error occurs.

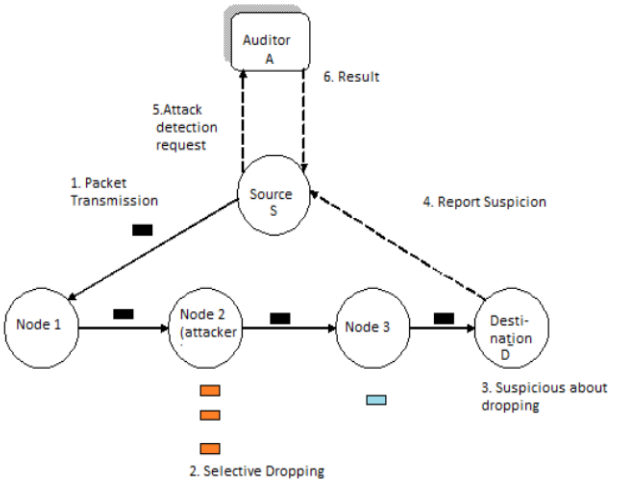


Figure 3.Architecture of Proposed Modeling

Optimized Link routing protocol is used to avoid link error or if it occurs OLSR helps to overcome the link error. Actually link error means, that the packet send by the source is transmitted through a specific route and, in some cases it leaves the route, so the destination doesn't receive the packet send by the source node. This problem can be overcome by OLSR, finds the route and sends it to HLA.HLA distributes different keys to all the nodes in the route. Now the nodes can transmitting the packet to the neighboring node by using the key, actually the node doesn't have any knowledge about the neighbors.

Various other processes are also implemented for different situations. The routing protocol is mainly used to detect the transmission errors in the program through which it can be determined. This type of routing concentration and process to be maintained in a protocol based dependencies. The protocol, based dependencies consist of a certain rules that should be formatted under a simpler concept of mechanism through which the network is defined. Those data transmitted at a rate of path of external issues and through which they can be formatted under the algorithm 1 should be used.

4.2. OLSR(with auto correlation)

The Optimized Link State Routing protocol (OLSR) is a routing protocol that is the most effective for mobile ad-hoc networks. OLSR is a proactive link-state routing protocol that contains a list of information that specify the node and its neighboring nodes, routing path between nodes, specifying number of packet transmission, time needed for packet transmission and so on. OLSR has less average node to node delay. The OLSR routing is both reactive and proactive methodology. The OLSR implementation is more user-friendly. It is using to auto-correlation mechanism. Because it is used to find the shortest path and high speed data transmission in the network. This protocol is used for the rapid changes of the source and destinations pairs. This protocol does not require any link for the control messages.

The Optimized Link-State Routing protocol can be divided in to three main modules:

- Neighbor sensing
- Multi-Point Relaying
- Link-State messaging and route calculation

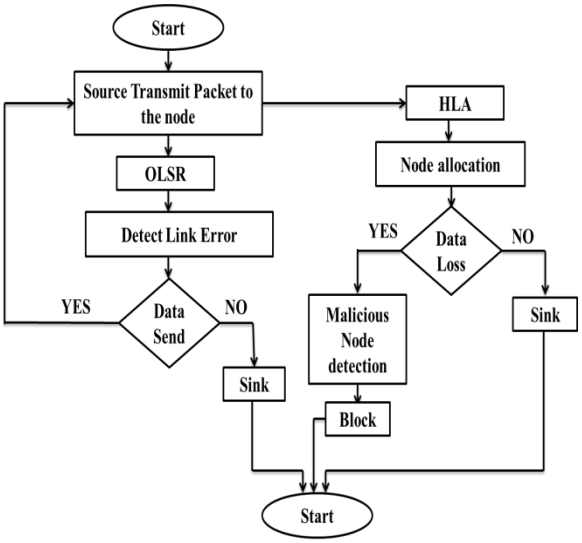


Figure 4. A Simple Flowchart

The main issue of the process can be declared in a simple flow chart as shown in the above Figure 4. Here the data transmission is started in a source area. Then the packet formation is used. And then the OLSR process is taken place by building the process in a various format to make the data transmission to overcome the link error. Another source of file can be used to process for the simple environment. This can be maintained under the source that should be used for various other hops to transmit the data. The proposed model successfully overcomes the link error. Then the next process is the data transmission to the sink. If the data is not properly transmitted the next process is to detect malicious node, and this process is done with the help of the HLA. Then the data are transmitted to the sink node.

4.3. Algorithm Used For Data Privacy

Ceaser cipher algorithm is used for data privacy. This algorithm includes three steps:

1. Key generation

2. Encryption

RESEARCH ARTICLE

3. Decryption.

1. Key generation is done with the help of HLA.

2. The original message T_i is encrypted by following procedure

$C_i=(T_i+k)(\text{mod } m)$

Ci is a cipher text

3. The original message T_i is decrypted by reverse procedure

$T_i=(C_i-k)(\text{mod } m)$

This algorithm shown in below

Ceaser cipher

If(character in alphabet)

{

If(character is in bottom half of packet

[A- M| a-m])

Character=character+13;

Else/* character is in top half [N-Z |n-z])*/

Character=character-13;

}

Print (character);

The encryption can be described with following formula

$C_i=(T_i+k)(\text{mod } m)$

C_i=ith character of the closed text

T_i=ith character of open text

K=shift

M=length of alphabet

The process of decryption uses reverted procedure

$T_i=(C_i-k)(\text{mod } m)$

Algorithm 1: Ceaser Cipher

5. RESULTS AND DISCUSSION

5.1 Packet Delivery Ratio

Table 1. Packet Delivery Ratio in Existing System

Number of packet transmission	Packet delivery ratio in existing system		
	AODV (%)	RIP (%)	OLSR (%)
10	0.6	0.4	0.4
20	0.5	0.3	0.4
50	0.4	0.2	0.3

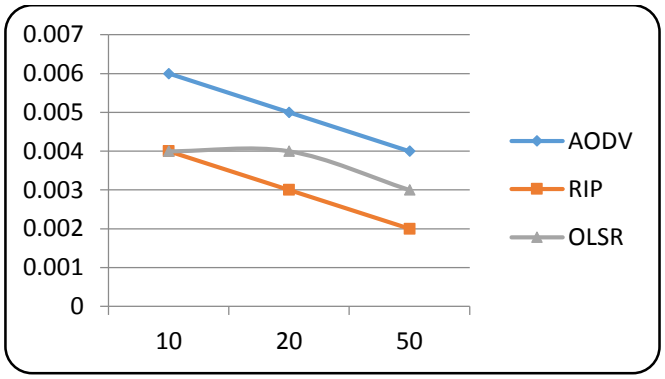


Figure 5. Packet Delivery Ratio in Existing System

Figure 5 and Table 1 describe the packet delivery ratio of existing system. If 10 packets are transmitted using AODV the packet delivery ratio is 0.6% it is higher than RIP and OLSR because the packet delivery ratio of RIP is 0.4% and OLSR is 0.4%.So in existing system packet delivery ratio of AODV is higher than RIP and OLSR. The calculation format can also be required for the above mechanism which are derived below.

$$Throughput=\frac{Numberofpacketsrecieved}{NetwortkOperationTime}$$

Table 2.Packet Delivery Ratio in Proposed System

Number of packet transmission	Packet delivery ratio in proposed system		
	OLSR (with auto correlation) (%)	AODV (%)	RIP (%)
10	0.93	0.7	0.43
20	0.75	0.62	0.34
50	0.8	0.48	0.22

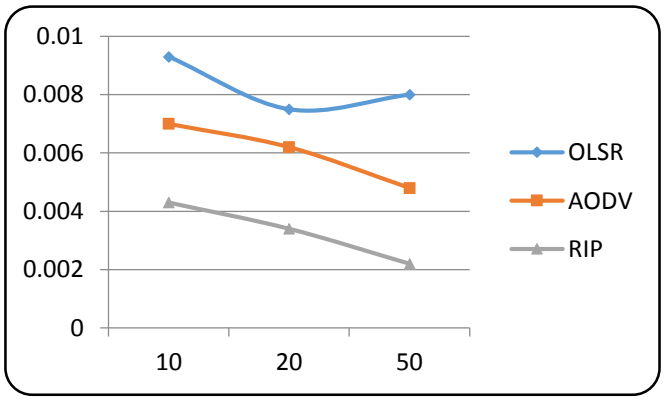


Figure 6.Packet Delivery Ratio in Proposed System

RESEARCH ARTICLE

Figure 6 and Table 2 describe the packet delivery ratio of this research work. If 10 packets are transmitted using OLSR with auto correlation mechanism, the packet delivery ratio is 0.93% it is higher than AODV and RIP because the packet delivery ratio of RIP is 0.4% and AODV is 0.6%. Here OLSR has highest packet delivery ratio because of using an additional mechanism called auto correlation. So in this research work the packet delivery ratio of OLSR is higher than AODV and RIP.

Table 3. Comparing Packet Delivery Ratio of OLSR (With Auto Correlation) and AODV in Proposed Model

Number of packet transmission	Packet delivery ratio	
	OLSR (with auto correlation) (%)	AODV (%)
10	0.93	0.7
20	0.75	0.62
50	0.8	0.48

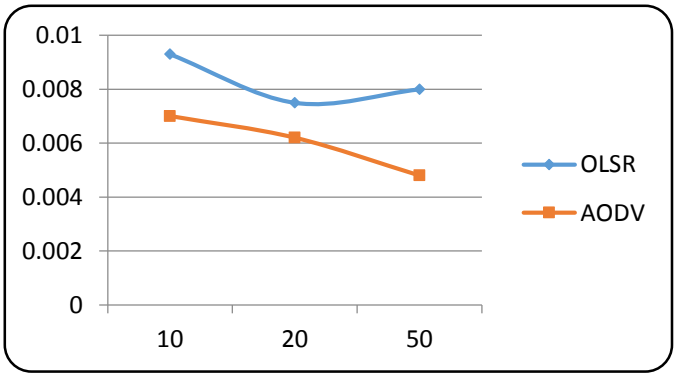


Figure 7 Comparing Packet Delivery Ratio of OLSR (With Auto Correlation) and AODV

Figure 7 and table3 describe the comparison of packet delivery ratio in OLSR(with auto correlation) and AODV .When compared to AODV packet delivery ratio of OLSR is high because of using auto correlation mechanism.

Table 4. Comparison of Packet Delivery Ratio Proposed OLSR with Auto Correlation and Existing OLSR without Auto Correlation

Number of packet transmission	Packet delivery ratio	
	Proposed OLSR (with auto correlation) (%)	Existing OLSR (without auto-correlation) (%)
10	0.93	0.4
20	0.75	0.4
50	0.8	0.3

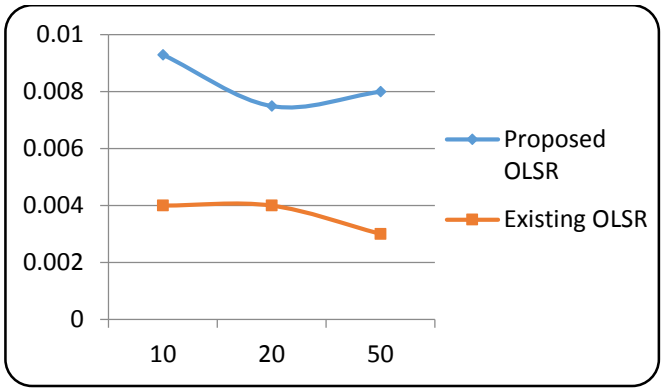
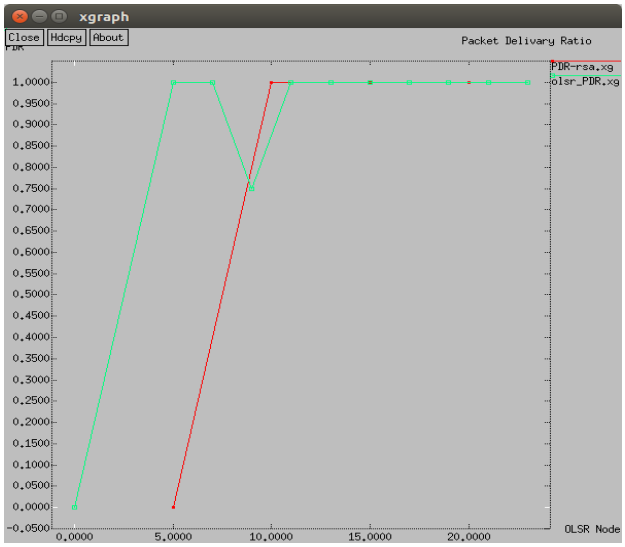


Figure 8 Comparison of Packet Delivery Ratio Proposed OLSR with Auto Correlation and Existing OLSR without Auto Correlation

Figure 8 and table 4 describe the comparison of packet delivery ratio in proposed OLSR (with auto correlation) Routing and existing OLSR (without auto correlation) Routing .Here in this research work OLSR has highest packet delivery ratio because using auto correlation mechanism. The packet delivery ratio of OLSR is higher than existing OLSR (without auto correlation) routing.

Figure 9 Packet Delivery Ratio



The main usage of the proposed mechanism is to implement the simple and efficient process for detecting the data packet in the network. We have to find the delivery ratio of the packet by using the number of packets in the system. And also it is used to detect the number of losing packets held in the network. That is the simple and efficient process through which the data can be maintained in the Figure 9. The comparison is taken place in the proposed OLSR and the existing AODV data. Among that the OLSR graph maintains the simple processing mechanism.

RESEARCH ARTICLE

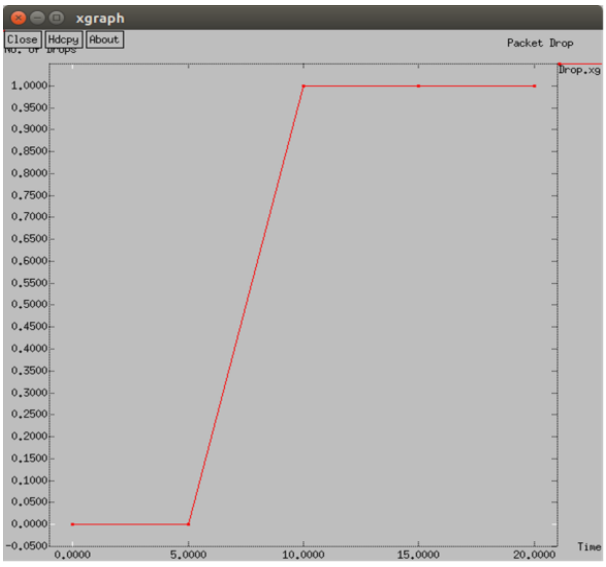


Figure 10.Detecting Packet Drops

The above Figure 10 describes detects the packet drops. In OLSR the packet drops are low when compared to AODV and RIP because in OLSR we use auto correlation mechanism. Which considerably reduces the packet dropping in an efficient way. This should be processed in different format. To maintain in a simple and efficient from of the source through which it can be determined.

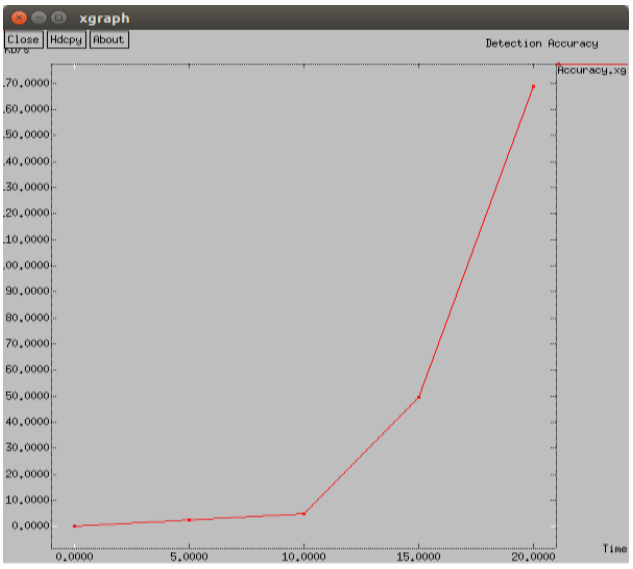


Figure 11.Detection Accuracy

The above Figure 11 describes the detection accuracy of OLSR. In OLSR detection accuracy is high. It will detect the malicious nodes and link error with high accuracy, when compared to RIP and AODV. Therefore, in this research work the time delay for detecting the malicious node and link error is reduced.

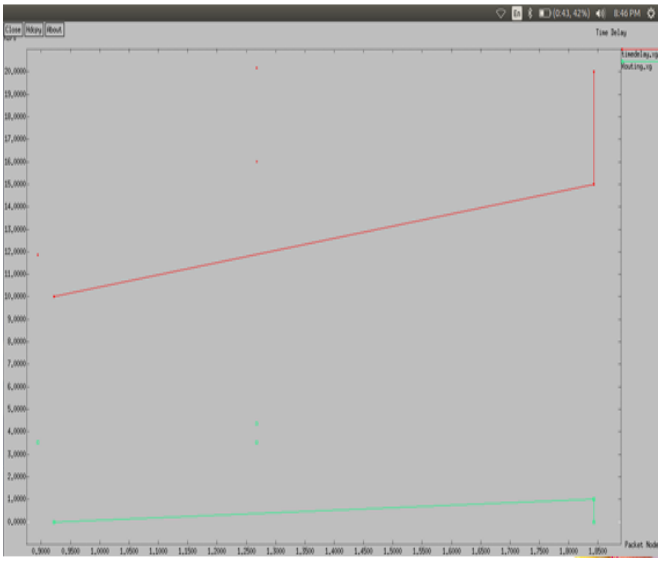


Figure 12 Comparison of Time

Figure 12 describes the timing details of existing and proposed research work. Time is reduced in the proposed model when compared to existing model because of using OLSR with Auto correlation mechanism. By using this mechanism the shortest path between source and destination is easily identified.

6. CONCLUSION

Wireless Sensor Network (WSN) suffers from link error and packet dropping. The characteristics of routing protocols AODV, RIP and OLSR are studied and further we modified the OLSR protocol with auto-correlation mechanism to perform well than the other existing protocols. Implementation of auto-correlation mechanism is OLSR will find the shortest path and high speed data transmission can be carried out in the network environment. The anchor node selection is also implemented in the research work. The anchor node is used to detect the packet dropping and link error using auto -correlation mechanism. Thus, proposed model performs well than the existing models on the basis of computation time and communication overheads. Further, we compared the performance of proposed OLSR (Auto-correlation mechanism) with the existing protocols such as AODV, RIP and OLSR. It has been noticed that the proposed modified OLSR protocol outperforms than the other protocols.

REFERENCES

[1] K. Gaj and P. Chodowiec, "FPGA and ASIC Implementations ofAES," Cryptographic Engineering, pp. 235-294, Springer, 2009.
[2] A. Shamir, How to Share a Secret, Communications of the ACM, 22(11): 612-613, November 1979.
[3] L. Lamport, Password Authentication with Insecure Communication,Communications of the ACM, 24(11): 770-772, November 1981.
[4] A. J. Menezes, P. C. van Oorschotand S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, October 1996.

RESEARCH ARTICLE

[5] H. Deng, W. Li and D. P. Agrawal, Routing security in wireless adhoc networks, IEEE Commun. Mag., 40(10): 70-75, October 2002.
[6] Biswas, Suparna, and Subhajit Adhikari. "A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network."International Journal of Computer Applications 131.17 (2015): 28-35.
[7] Ramakrishnan, B., R. S. Rajesh, and R. S. Shaji. "An efficient vehicular communication outside the city environments." International Journal of Next-Generation Networks (IJNGN) Vol 2 (2010).
[8] B.Ramakrishnan.,M.selvi,R.BhagavanthNishanth "Efficient Measure Of Routing Protocols In Vehicular Ad Hoc Networks Using Freeway Mobility Model", Wireless Networks, PP: 1-11 (2015).
[9] Ramakrishnan, B. "Performance analysis of AODV routing protocol in Vehicular ad-hoc network service discovery architecture." *Network* 13.14 (2009): 65-72.
[10] Joe, M. Milton, B. Ramakrishnan, and R. S. Shaji. "Modeling GSM based network communication in vehicular network." International Journal of Computer Network and Information Security 6.3 (2014): 37.
[11] TaoShuand Marwan Krunz,"Privacy Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Adhoc Networks",IEEE Transactions on Mobile Computing, Vol.14,no.4,April 2015.
[12] B.Awerbuch,R.Curtmola,D.Holmer,C.Nita-Rotaru, and H.Rubens, "ODSBR: An on demand secure byzantine resilient routing protocol for wireless ad hoc networks",ACMTrans.InformSyst.Security,vol.10.no.4,pp.1-35,2008.
[13] K.Balakrishnan, J.Dengand, P.K.Varshney, "TWOACK Preventing selfishness in mobile ad hoc networks," in Proc. IEEEWirelessCommun Network Conf., 2005, pp.2137-2142.
[14] E.GerhardsPadilla,N.Aschenbruck,P.Martini,M.Jahnke and J.Tolle. "Detecting Black Hole Attacks in Tactical MANETs using Topology Graphs", InProc. Of the 33rd IEEE Conference on Local Computer Networks (LCN), Dublin,Ireland, and October 2007.
[15] Daş, R., Karabade, A., Tuna, G., (2015), "Common Network Attack Types and Defense Mechanisms", IEEE 23. Signal Processing Applications Conference (SİU-2015), 16-19 May 2015, InonuUniversity, Malatya.
[16] W.Yu,Y.Sun and K.R.liu ,HADOF:Defense Against Routing Disruptions in mobile ad hoc networks,InProc.24thIEEEINFOCOM,Miami,USA,March 2005.
[17] Ramakrishnan, B., S. R. Sreedivya, and M. Selvi. "Adaptive routing protocol based on cuckoo search algorithm (ARP-CS) for secured vehicular ad hoc network (VANET)." International Journal of computer networks and applications (IJCNA) 2.4 (2015): 173-178.
[18] Merlyn, A. Anuba, and A. Anuja Merlyn. "Energy Efficient Routing (EER) For Reducing Congestion and Time Delay in Wireless Sensor Network." International Journal of Computer Networks and Applications 1.1 (2014): 1-10.
[19] Baykara, M., Daş, R., (2015)."A Survey on Potential Applications of Honeypot Technology in Intrusion Detection Systems", International Journal of Computer Networks and Applications (IJCNA), 2(5), 203-211.
[20] Shaji, R. S., R. S. Rajesh, and B. Ramakrishnan. "An Efficient Routing scheme for reliable path establishment among Mobile Devices in Heterogeneous Networks", International Journal of Computer Science and Information Technologies, Vol. 1 (5) , 2010, 355-362.
[21] Namesh, C., and Dr B. Ramakrishnan. "Analysis of VBF protocol in Underwater Sensor Network for Static and Moving Nodes." International Journal of Computer Networks and Applications 2.1 (2015): 20-26..
[22] Nishanth, R. Bhagavath, B. Ramakrishnan, and M. Selvi. "Improved signcryption algorithm for information security in networks." International Journal of Computer Networks and Applications (IJCNA) 2.3 (2015): 151-157.
[23] Karadogan, İ., Daş, R., (2015). "Analysis of Attack Types on TCP/IP Based Networks via Exploiting Protocols)", IEEE 23. Signal Processing Applications Conference (SİU-2015), 16-19 May 2015, İnönü Üniversitesi, Malatya.

Authors

M. Kavitha received her B. Sc Mathematics from Muslim Arts College, Tiruvithancode affiliated Manonmanium sundaranar University, Tirunelveli, India and MCA degree from Anna University, chennai. Presently she is a research scholar in Department of Computer Science and Research Centre, S. T. Hindu College, Nagercoil, India. Her Research interests include cloud computing, MANET.

B. Ramakrishnan is currently working as Associate Professor in the Department of Computer Science and research centre in S. T. Hindu College, Nagercoil. He received his M. Sc Degree from Madurai Kamara jUniversity, Madurai and received M. Phil (Comp. Sc) from Algappa University Karaikudi. He earned his Doctrate degree in the field of Computer Science from Manonmanium Sundaranar University, Tirunelveli. He has a researching experience of 29 years. He has twelve years of research experience and published more than fifty research articles unrepeated international journals. His research interests lie in the field of vehicular networks, mobile network and communication, cloud computing, Green Computing, Ad-hoc Networks and Network Security.

Resul Das received his BS and MSc. in Computer Science from Firat University in 1999, 2002 respectively. He received PhD degree from Electrical and Electronics Engineering Department in same university in 2008. He is an Assoc. Professor at the Department of Software Engineering of Firat University, Turkey. He has authored several paper in international conference proceedings and refereed journals, and has been actively serving as a reviewer for international journals and conferences. His current research interests include Knowledge Discovery, Web Mining, Complex Networks, Computer Networks, Information and Network Security.