INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

OPTIMIZING SECURITY ISSUE OF OLSR ROUTING PROTOCOL BASED ON TRUST METHOD IN WIRELESS SENSOR NETWORKS

Bahram Najafpour[1], Behzad Mahdavi[2], Parisa Soleimani[3], Rozbeh Rahmani[4]

[1]Department of Computer, Novin Institute of Higher Education – Ardabil - Iran.
[2,4]Department of Computer, Ardabil Branch, Islamic Azad University, Ardabil, Iran.
[3]Photonics Group, Research Institute for Applied Physics and Astronomy, University of Tabriz, Tabriz, Iran.

Author Correspondence: Iran, +989398444054, b.najafpour@E.novin.Ardebil.ac.ir

Abstract: - The networks wireless sensor has attached much attention recently due to the wide applications in military, civilian, wildlife monitoring and disaster management. The nature of the networks wireless sensor makes it be vulnerable against attacks. In the wireless network sensor, making decisions has been essential for doing special tasks to work as an aid in communication in wireless sensor networks. To assist this process, trust management systems can be affected. In this paper, a protocol based on the trust system proposed a perfect solution for sensor networks to provide high security. Simulation results shows that the proposed protocol B-OLSR performs better in terms of the number of packets dropped, the number of lost packets and the throughput rate toward the OLSR routing protocol.

Keywords: Trust management, OLSR, B-OLSR, Routing Protocol, WSNs.

1. Introduction

Authors Recently, the networks wireless sensor has been attached much attracted due to the wide applications in military, civilian operations. Many of crucial network tasks have critical roles, thus the security must be considered at designing time. Wireless sensor networks are vulnerable to security attacks related to the wireless infrastructure. This gets worse because they work in an environment without infrastructure. Because of it all the network functions such as routing nodes is done with the partner of other nodes. It means that all nodes act as routers and the generated packet by sink nodes are sent to neighbours on their way. It makes malicious node (regardless of the type of operations) affect the operation of the network [1] [2].
To deal with, the attacks has been proposed an approach dependence on human societies which are nodes on the behaviour of their neighbours which to assess the reliability of their According to certain aspects of the behaviour trust metric is called trust metric. The nodes are creating trust relationships between themselves and routing decisions not only in terms of geographical information or other routing weak information but also they are the based on their predictions contribution honest neighbours (or just trust them) [3].

In this work we consider the OLSR routing protocol and the protocol by adding trust management techniques, a new protocol has been proposed which is called B-OLSR that improves network performance in terms of the number of dropped packets, number of packets lost and packets improves throughput rate.
The remainder of the paper is organized as follows: In section 2, the related work has been discussed in section 3, 4 trust management in WSNs and OLSR routing protocols has been studied, respectively. In section 5 attacks on the OLSR routing protocol is presented. Section 6 also includes the authentication and encryption in wireless networks. In sections 7 and 8 the proposed scheme and simulation results are discussed. Finally, in section 9 the conclusion is explained.

2. Related works

In this section, we are going to discuss trust management in wireless networks with the advantages and disadvantages.

2.1. TARF

TARF technique achieves the multipath routing in wireless sensor networks by evaluating the reliability of node neighbouring. It indicates unreliable nodes and orbits in the routing. This method focuses on energy efficiency, reliability and Attacks which an attacker perform it on the network traffic and routing information by repeating the false impersonation. The advantage of this method is that it does not need severely concurrency limits and geographical information. It is implemented as a module in tiny OS by low overhead and can be embedded in minimal effort on existing routing protocol. This method targets are high-throughput, energy efficiency and scalability. If it detects an error node in the path, the path will build scratch.

2.2. Trusted AODV

This protocol [5] is AODV developed known protocol which is proposed by Xiaoqi Li and et al for taking the routing metrics of trust. Firstly, the trust mechanism is introduced, and then changes the rules of the routing by considering the reliability of AODV routing. Particular emphasis of this approach is that a set of guidelines is derived for a node which is updating their opinion about other nodes by regarding them. Thus, a data mechanism exchange of trust is designed for networking applications when it makes use of trust model application. Specially, the trust proposed processes, trust judgment and updating on the development of routing tables, the development of routing messages and route discovery are defined based on trust.

2.3. TEAODV

TEAODV Protocol [6] is a routing protocol based on trust-aware of energy which is created by adding trust to routing aware of EAODV energy. It is perfectly similar to trusted AODV protocol, but instead of EAODV is used are used. In this protocol both nodes trust and confidence are used. The trust by each node for each routing is calculated in its routing table and the levels of trust depend that a packet can reach its destination. Trusted node confidence values is calculated based on the difference between the advertised destination node and confidence started to transfer current. Then, these values are used in the routing decision.

2.4. TLSRP

TLSRP Algorithm [7] is a new algorithm to construct a reliable source to sink nodes which is presented the direct and indirect trust. Trust according to nth root is calculating node service features quality and suggested experience by its neighbours. This model is a modified LSR protocol. This resistance has not been evaluated against various attacks.

2.5. ATSR

ATSR Algorithm [8] is a fully distributed algorithm to assess the reliability of node. According to the algorithm, nodes by considering the criteria of specific trust control their neighbours' treatment and a direct trust value is calculated for each neighbour's node. ATSR uses indirect trust too. Then, it combines these two values to obtain the total trust.

2.6. TRUSTEE

TRUSTEE Algorithm [9] is suggested as a method based routing trust in sensor networks with constraint energy. This method is a flexible and practical way to evaluate the quality of the path. Then, it chooses the path which is best meet security requirements. It assumes that each node contains information about neighbour nodes and to secure neighbours connection share keys together through the key pre-distribution method.

The method not only consumes resources such as memory, energy and computational overhead can be minimized, but also could work well due to the node authentication against external attacks and it is able to defend against chosen attack. As a result, the network throughput is greatly enhanced. In [10] a distributed trust model is presented for a sensor network environment. the method is a distribution function and the calculation function has a cost that makes use of the trust, energy and location information, which is applied for routing decisions and has two advantages: Firstly, by controlling the different aspects of behaviour, it provides defence against wide variety of attacks (Unlike many of the techniques, which is presented trust, which is employed a few measures), Second is energy-aware and as a result can help to load balancing traffic and more resistance to attacks.

2.7. TDSR

Trust Aware Dynamic Source Routing [11] secure routing DSR protocol, a mechanism of modules "watchdog" and "Path-rater" has been designed in routing protocol. The method is utilized in protocol routing which the source determines the path of the packets. Watchdog is responsible for detecting selfish nodes that do not send packets. In this method, each node in the network is holding every packet in their buffer for a limit time. During this time, the wireless interface is in promiscuous mode for listening and understanding that each node sends either the packet to the next node or not. Path-rater attributes based on the received feedback from the watchdog to the different degree of node. Then, degrees are used to choose routes with the highest degree nodes. This method improves the resulting security as the same as the TAODV method. Although, it is not able to deal with all the attacks.

2.8. CONFIDANT

CONFIDANT [12] is a trust management system which is adds a Reputation system to approach watchdog and Path Rater. Trust management events have been managing published events by the watchdog technique and have been emitting warning alerts to other groups in relation to malicious nodes. Alert recipients are kept in a list called friend-list which is configured through the user to user authentication mechanism.

Reputation system keeps a black list at each node maintains and it shares by the existence group in friend's list. CONFIDANT protocol based on a punishment is applied by do not sending packets of nodes that trust level is lower than a threshold value.

2.9. CORE

CORE Protocol [13] is similar to CONFIDANT. However, it uses the reputation of a complex exchange system used. CORE reputation of a node is divided into three separate components. The direct reputation is obtained from personal observation; indirect reputation is a positive report by another nodes and Functional reputation based on monitoring the behaviour during a particular task. The total amount of fame to get fame is combined with a weighted mode.

2.10. Trusted GPSR

Trusted GPSR method [14], GPSR algorithm is developed to consider the trust. To do this whenever a node sends a packet, it waits until the packet is intercepted by their neighbours. Then, the node Based on this information (Send fast and immediately) keeps a trust for the maintenance of its neighbours. Then, the information is used in routing decisions.

2.11. TRANS

TRANS [15] is a routing protocol to avoid unsafe places. The protocol chooses routes between nodes not only based on trust information the number of steps, but also chosen by using of other measure. This protocol is based on the assumptions that sensors knowing their approximate location which uses in geographic routing (e.g., GPSR). The TRANS a trusted neighbour sensors that can decode the request and sufficiently reliable

(Given the history of recorded Posts by sink nodes and intermediate), a sink sends messages only to trusted neighbours (Nodes that trust value greater than the threshold). Similarly, neighbours and their neighbours reliably send packets to the closest place to have a destination.

Therefore, the packets reach their destination through the path of trusted sensors. One of the importance features of TRANS is that creating a blacklist is well distributed by sink. This is due to the assumption that the sink node will not be in danger. Sink with the observed response is specific misbehaviour, misbehaviour explore potential areas that are isolated and insecure areas. After removing the package in a high level, sink will start to search for unsafe places along the route. With the discovery that places them up and give this information to neighbouring nodes.

2.12. SPINS

SPINS is a set of optimized security protocols for sensor networks to provide data confidentiality, which is proved two-way authentication and data confidentiality. However, in relation to denial of service attacks or compromised node does not perform a specific job and just to ensure that a compromised node network reveals no keys.

3. Trust management in wireless sensor networks

One approach is proposed to deal with attacks on wireless sensor networks, which is derived from human who the nodes on the behaviour of their neighbours are supervising in order to assess their reliability according to the particular aspect of behaviour that is called trust metrics. Accordingly, nodes provide trust relationships between themselves and routing decisions are not only in terms of geographic information or other poor routing information, but also are based on their predicted contribution of honest neighbours (or the same amount of trust towards them). In other words, it is implemented a trust management system.

The key distribution based on methods can be used to maintain data integrity and also robust encryption and authentication methods and powerful tools are closed to protect the authenticity and validity of the accuracy of the nodes. However, they were unable to identify a large set of routing attacks such as selfish behaviour, Selective Forwarding Attack, Black hole and so on. A trust model is used for higher layers such as routing decisions, and data aggregation for selecting the cluster heads or key distribution. Trust management techniques are a powerful tool to detect unexpected behaviour node (malicious nodes or nodes with damage). When was identified misbehaviour nodes, their neighbours can use the information as a non-participating to send data, data aggregation and other participate activities. The power of trust is more than traditional encryption techniques and they could solve problems which they could not solve them. For example, they can solve judgment problems related to the behaviour of the sensor nodes.

It needs trust management to create secure and reliable applications for sensor networks. Since sensor networks have unique challenges, it cannot use the trust models for other network. Thus, new solutions are needed to deal with security attacks. In fact, trust is in the amount of Si nodes, which is Sj on cooperation between i and j nodes, behaves as predicted. To evaluate the reliability of a node to its neighbours or to monitor its behaviour (Direct observation) or may communicate with other nodes to exchange their observations. Trust and define methods to obtain information on the reliability of each node, called a trust model.

The main purpose of a sensor network is increasing throughput and improves security, stability and longevity of the network even in the presence of attackers. Establishing Trust in agency-based distribution network, Trust models can be divided into centralized and distributed models. Centered at a node is deemed reliable, Decisions on trustworthiness of nodes, based on data collected from a personally who has made or data received from other nodes, it undertakes. The main advantage of this approach is that the nodes can monitor the behaviour of all nodes in the nodes is regarded as the most powerful; this reduces the need to monitor the network remains. However, this method has the problem of single point of failure. Architecture can be replaced by a trust organized networks of clusters and cluster heads should be assigned to the monitoring agency. The trustworthiness of each node in the cluster heads will be considered for selection. In the decentralized case, each node monitors the behaviour of its neighbours and Based on the collected metrics to measure their reliability and is used in routing decisions. The establishment of trust and cost to implement is distributed the same functionality in the network. Different aspects of behaviour can be monitored in a wireless sensor network. Monitor specific aspects of behaviour makes the diagnosis of various security attacks.

4. OLSR Routing Protocol

OLSR protocol is a proactive protocol, which uses an optimized flooding mechanism to diffuse partial link state information to all network nodes. The protocol uses multi-point relays (MPRs) which are selected nodes that forward broadcast messages during the flooding process. The link state information is generated only by nodes elected as MPRs and each MPR must only report on the state of links between itself and its selectors. Two types of control messages, HELLO and TC, allow each node to obtain and declare network topological information [30].

Hello messages which are sent as broadcast to all neighbour nodes (nodes which are in radio range of the sending nodes). Messages have contained a list of the source node's neighbours with the status of their relationship and two operations are performed: Adjacent nodes identify two-step of the network topology and will ensure neighbour activation link [20].

4.1. MPR nodes

OLSR protocol Optimized the Link state algorithm, it is based on a series of information are selected as Multipoint Relay (MPR). The task of MPR sending messages nodes are selected during the flooding. Nodes indicate their MPRs in the Hello Message with Placing MPR field in the link status. Neighbouring nodes of a node which has selected the node as MPR, MPR selectors that are called nodes. MPR selectors at regular intervals about MPR selector their status and link them using TC messages are released throughout the network and nodes uses this information to calculate routes.

4.2. Evaluate the Topology control messages generated

If selected MPR (i) topology control massages did not correctly produce MPR's selection, each (j) selector should supposed to be bad MPR when it is done according to formula 1:

$$i \in MPRS_j, \left(j \overset{TC_i}{\leftarrow} i\right) or \left(j \overset{TC_i}{\leftarrow} i, j \notin TC_i\right) \quad (1)$$

$$\Rightarrow j \neg trusts\,(i)$$

4.3. Evaluate the topology control messages and data packets

If selected MPR (i) do not send data packets ($DATA_X$) and topology control messages (TC_X) has been sent by selected MPR, each selector (j) MPR is supposed to be bad when it is done according to formula 2:

$$i \in MPRS_j, \left(j \overset{TC_j}{\rightarrow} *, j \overset{(TC_j)_i}{\leftarrow} i\right) or \left(j \overset{DATA_j}{\longrightarrow} *, j \overset{(DATA_j)_i}{\leftarrow} i\right) \quad (2)$$

$$\Rightarrow j \neg trusts\,(i)$$

In figure 1 and 2 are shown the mechanisms of classical broadcast and mechanism using MPR broadcast, respectively.

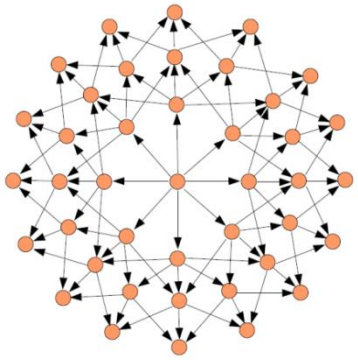

Fig 1: Regular flooding

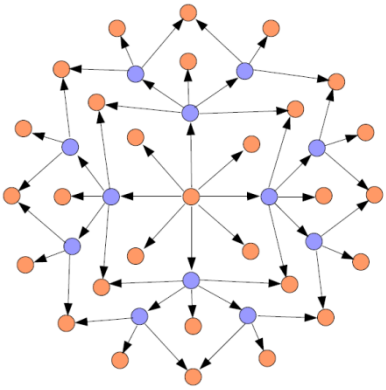

Fig 2: MPR flooding

5. Attack on OLSR

In an environment without infrastructure networks, sensor nodes for routing and forwarding their packets to the base station rely on partnerships between themselves. Many of the special attacks target routing processes. For example, the black hole attack, a node indicates selfish treatment and avoids sending the same traffic to its neighbours. In addition, it could be worse when the situation cannot send any traffic, crossing their paths in order to capture network traffic. Another series of attacks that are based on packet switching (routing packets or data packet) which can devastate Routing process and cause faulty nodes for routing traffic or it can damage the received data to the sink. Another type of attacks, including a Sybil attack which node has feigned features and wormhole attacks, which more than one node in order to capture data transmitted or merely disrupt the routing process of working together.

5.1. Fabrication attacks on the OLSR protocol

Our proposed protocol was used to test fabrication attack. In this attack, the attacker node wants to select as a MPR node. It provides a HELLO message and sends to all the nodes which is received a HELLO. These messages are sent to the addresses used in a symmetric link [26]. In figure 3 before the attack, B chooses C as MPR for transmitting data to D. After the attack, the attacker node has three neighbours, but real and lying are several other neighbours. Neighbour nodes attacker when they observed attacker node has more neighbours of the faulty node is selected as MPR. It also assumes that the attacker node is the closest route to D, That's choosing why the attacker nodes sending data to D node. The attacker nodes A and B and C are trusted nodes for routing data to win to node D. While there is no evidence that the attacker nodes associated with the node D is absent. But in fact there is no paths between attacker and D and the other nodes have the confidence to take the attacker.

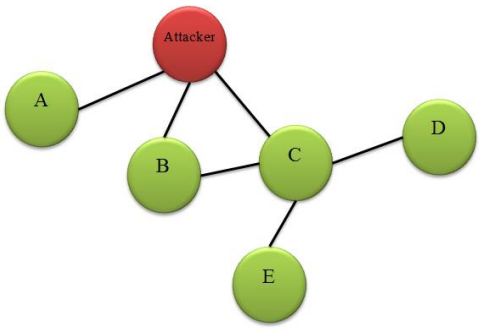

Fig 3: Fabrication attack

6. Authentication and data encryption

Typically, classic network security occurs through authentication and encryption. Broadcast authentication is a critical security service in wireless sensor networks. Collaboration between neighbouring nodes can lead to sabotaged provide accessible routes along the tunnel and routing messages between them. Wormhole attack can also occur with the cooperation between the two nodes. According to the node authentication by signatures, it is

impossible to occur Table overflow and black holes attacks. The technique can be considered as a first line of defense because they are preventative technique but they cannot create a complete security framework for sensor networks. In fact, by using of these techniques, cannot prevent a compromised node in the network which is a part of the authentication and to perform any act contrary.

7. Proposed protocol

This is the way that each node periodically sends a trust message to its neighbours. This message will be given to the neighbouring nodes need to apply changes to this data. The changes must be based on the protocol. Nodes modified data are broadcast to neighbours. Every neighbourhood has been modified and the original sender of the message will see the modified trust. Given that the original data had been observed the trust message sender can be trusted to make decisions.

All nodes start with 100% confidence but whenever the trust message sender does not receive the modified trust neighbours or received a modified trust by incorrect data, the confidence decrease as much as 25%. The measure which takes into account in the trust message is a random number. These data were selected because of the low overhead; it can be used from any other data type. When the trust of each node has been zero, the node is blocked by other nodes and places on their black list.

8. Analysis and simulation results

The proposed protocol simulation experiments have been performed by using of network simulator ns-allinone-2.34. In this section, we compare our proposed protocol OLSR and OLSR protocol type of traffic which is using CBR. It is compared dropped packets, packet loss and throughput rates. The used parameters for simulation are shown in Table 1.

Table 1. Experimental Parameters

Simulator	ns-2.34
Comparison	OLSR and B-OLSR
Mac type	Mac/802.11
antenna	Omni antenna
Network interface type	Phy/wirelessphy
Simulation time	2060 s
Packet size	1000 byte
Traffic model	CBR
No. of nodes	50
No. of malicious nodes	3, 6 and 9
Mobility	fixed
Network size	250 m×250 m

Figure 4 shows the number of dropped packets between the two protocols and shows the 3 malicious nodes in the network. Simulation results shows that the number of dropped packet in the OLSR protocol is about 7862 but in the proposed protocol reduced to 6171 packet.

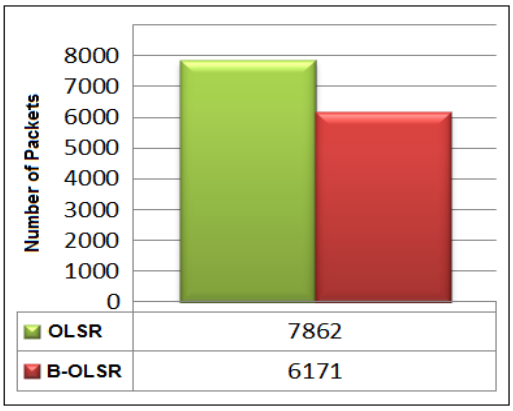

Fig 4: number of drop packets with 3 malicious nodes

Figure 5 shows the number of dropped packets between the two protocols and the 6 malicious nodes in the network show. Simulation results show the number of dropped packet in the OLSR protocol is 7430 but in the proposed protocol reduce to 6025 packet.

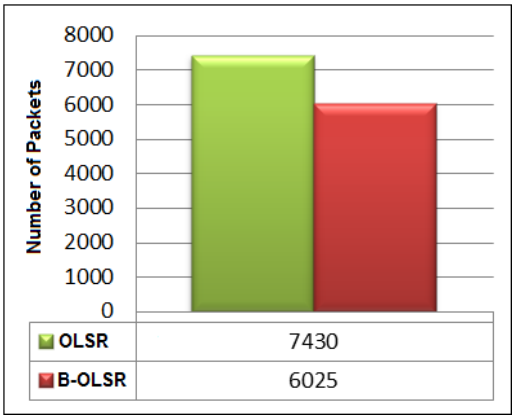

Fig 5: number of dropped packets with 6 malicious nodes

Figure 6 shows the number of dropped packets between the two protocols and the 9 malicious nodes in the network show. Simulation results show the number of dropped packet in the OLSR protocol is 7378 but in the proposed protocol reduce to 6560 packet.

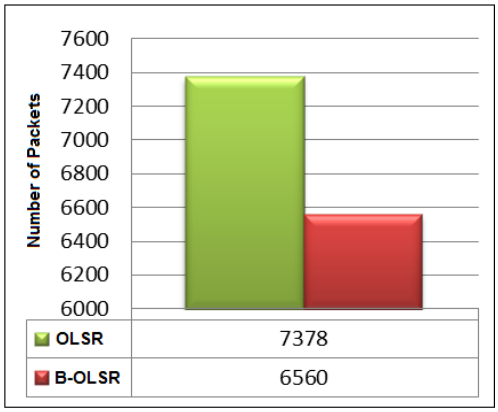

Fig 6: number of dropped packets with 9 malicious nodes

Figure 7 shows the percent of packets loss between the two protocols and the 3 malicious nodes in the network show. Simulation results show the percent of packets loss in the OLSR protocol is %17.8 but in the proposed protocol reduce to %9.62 packets.

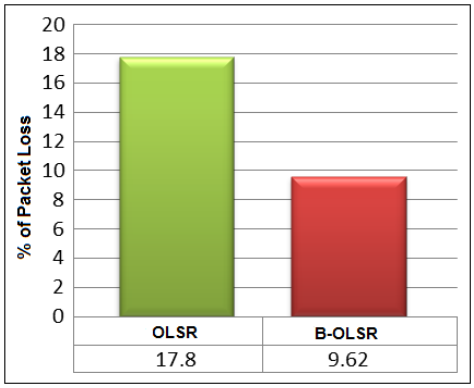

Fig 7: number of Packet Loss with 3 malicious nodes

Figure 8 shows the percent of packets loss between the two protocols and the 6 malicious nodes in the network show. Simulation results show the percent of packets loss in the OLSR protocol is %33.65 but in the proposed protocol reduce to %9.32 packets.

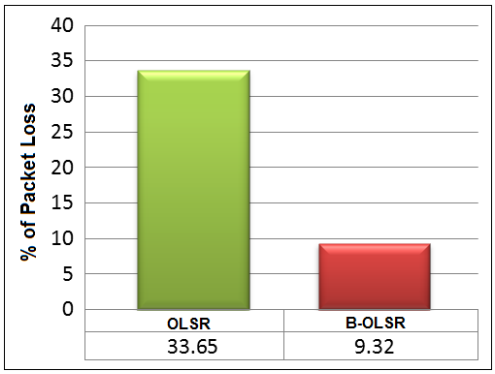

Fig 8: number of Packet Loss with 6 malicious nodes

Figure 9 shows the percent of packets loss between the two protocols and the 9 malicious nodes in the network show. Simulation results show the percent of packets loss in the OLSR protocol is %16.9 but in the proposed protocol reduce to %10.21 packets.

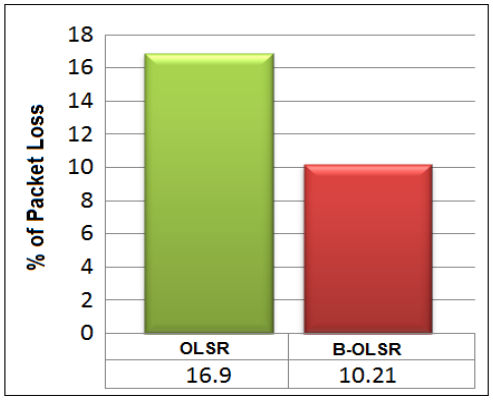

Fig 9: number of Packet Loss with 9 malicious nodes

Figure 10 shows the percent of Throughput between the two protocols and the 3 malicious nodes in the network show. Simulation results show the Throughput in the OLSR protocol is 1.34 but in the proposed protocol increase to %1.57.

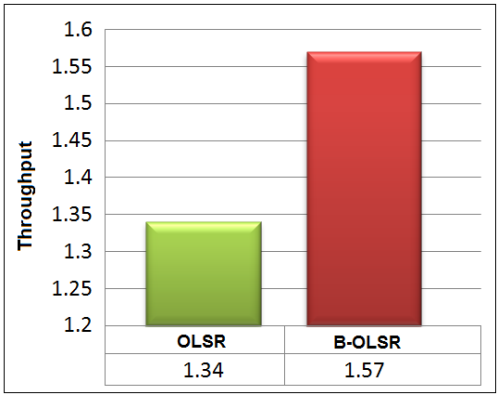

Fig 10: Throughput with 3 malicious nodes

Figure 11 shows the percent of Throughput between the two protocols and the 9 malicious nodes in the network show. Simulation results show the Throughput in the OLSR protocol is 1.28 but in the proposed protocol increase to 34.53.

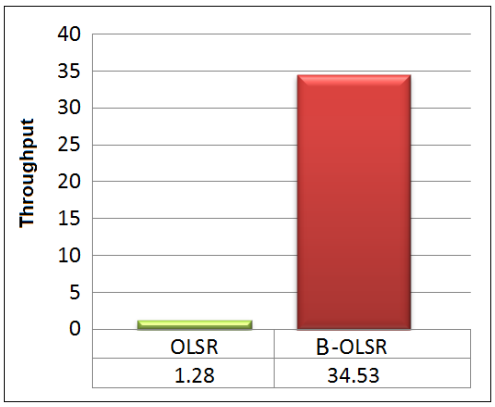

Fig 11: Throughput with 9 malicious nodes

9. Conclusion

In this paper, we studied the mechanism of OLSR routing protocol and the security issues of the protocol. In addition, we investigate the issues of trust management in the networks and we have shown how by the using of trust management, we can increase the secure of routing protocols for wireless sensor networks. We have introduced a new protocol that is called B-OLSR and with the Experiments and simulations have shown the proposed protocol in terms of three parameters: the number of packets dropped, the number of lost packets and the throughput rate channel is more efficient than OLSR protocol.

REFERENCES

[1] Yinying. Y, Mirela I. F, Mihaela. C, Improving network lifetime with mobile wireless sensor networks, Computer Communications 33, 0140-3664, PP.409-419, Elsevier (2010).

[2] Di Pietro, R., Oligeri, G., Soriente, C., Tsudik, G. (2013), United We Stand: Intrusion Resilience in Mobile Unattended WSNs, journal of IEEE Computer Society, ISSN:1536-1233, vol.12, Issue.7, PP. 1456 - 1468.

[3] Jin-Hee Cho, Swami, A., Ing-Ray Chen (2011), A Survey on Trust Management for Mobile Ad Hoc Networks, journal of IEEE Communications Society, ISSN:1553-877X, vol.13, Issue.4, PP. 562 - 583.

[4] AmirPirzada, A., Dattaa, Amitava., McDonald, C. (2006) Incorporating trust and reputation in the DSR protocol for dependable routing. Computer Communications, Vol.29, Issue: 15, PP. 2806-2821.

[5] AsadPirzada, A., McDonald, C. (2007) Trusted Greedy Perimeter Stateless Routing, IEEE.

[6] Buchegger, S., Boudec, J. (2002) Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes - Fairness in Distributed Ad-hoc Networks, Proceedings of the 3rd ACM International Symposium on Mobile Ad hoc Networking and Computing (MobiHoc). ACM Press, pp. 226 - 236.

[7] Marti, S., Giuli, T., Lai, K., Baker, M. (2000) Mitigating Routing Misbehaviour in Mobile Ad hoc Networks. Proceedings of the Sixth Annual International Conference on Mobile Computingand Networking (MobiCom), ACM Press, pp. 255-265.

[8] Michiardi, P., Molva, R. (2002) CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad hoc Networks, Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security, Vol.228, Kluwer Academic Publishers, PP.107 - 121.

[9] Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., and Culler, D. (2002) SPINS: Security Protocols for Sensor Networks. ACM Journal of Wireless Networks, 521-534.

[10] Sahil Babu, S., Raha, A., Kanti Naskar, M., (2011), Trustworthy Route formation Algorithm for WSNs, International Journal of Computer Applications, (0975 - 8887), Vol. 27, No.5.

[11] Samundiswary, P. (2012) Trust based Energy aware Reactive Routing Protocol for Wireless Sensor Networks, International Journal of Computer Applications (0975 - 8887) Vol. 43, No.21.

[12] Stelios, Y., Papayanoulas, N., Trakadas, P., Maniatis, S., Leligou, (2009) A Distributed Energy-Aware Trust Management System for Secure Routing in Wireless Sensor Networks, ICST Institute for Computer Sciences, Social-Informatics and Telecommunication Engineering.

[13] Tanachaiwiwat, S., Dave, P., Bhindwale, R., Helmy, A. (2004) Location-centric Isolation of Misbehaviour and Trust Routing in Energy-constrained Sensor Networks. IEEE International Conference on Performance, Computing and Communications.

[14] Weifangl, C., Xiangke, L., Changxiang, Shen, Shanshan, L., Shaoliang, P. (2006) A Trust-Based Routing Framework in Energy-Constrained Wireless Sensor Networks, Springer-Verlag Berlin Heidelberg.

[15] Xiaoqi Li, L., Jiangchuan, L. (2004) A Trust Model Based Routing Protocol for Secure Ad hoc Networks, IEEE Proceedings on Aerospace Conference, vol. 2.

[16] Zahariadis, T., Leligou, H., Karkazis, P., Trakadas, P., Papaefstathiou, I., Vangelatos C., Besson, L. (2010), Design and Implementation of A Trust-Aware Routing Protocol for Large WSNs, International Journal of Network Security & Its Applications (IJNSA), Vol.2, No. 3.

[17] Zhan, G., Shi, W., Deng, J. (2012) Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs, IEEE Transactions on Dependable and Secure Computing, vol. 9, No. 2.

[18] Fenye Bao., Ing-Ray Chen., MoonJeong Chang., Jin-Hee Cho (2012), Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection, ISSN: 1932-4537, vol.9, Issue.2, PP. 169 - 183.

[19] Xia, H., Jia, Z., Ju, L., Zhu, Y., (2012), Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory, ISSN: 2043-6368, vol.1, Issue.4, PP. 248 - 266.

[20] Toutouh, J., Garcia-Nieto, J., Alba, E., (2006), Intelligent OLSR Routing Protocol Optimization for VANETs, journal of IEEE Vehicular Technology Society, ISSN: 0018-9545, vol.61, Issue.4, PP. 1884 - 1894.

[21] Joshi, R.D., Rege, P.P., (2012), Implementation and analytical modelling of modified optimized link state routing protocol for network lifetime improvement, journal of IEEE Communications Society, ISSN:1751-8628, vol.6, Issue.10, PP. 1270 - 1277.

[22] Adnanea, A., Bidanb, C., de Júnior, R, T., (2013), Trust-based security for the OLSR routing protocol. ELSEVIER, journal of Computer Communications, Vol. 36, Issues 10 -11, June 2013, PP. 1159 - 1171.

[23] Huai Wu., Zhi Ren., Wei Guo., (2006), A MPR-flooding-based On-demand Routing Algorithm in Wireless Sensor Networks, Proceedings of the 2006 IEEE International Conference on Mechatronics & Automation, PP. 1937 - 1941.

[24] Nait-Abdesselam, F. (2008), Detecting and avoiding wormhole attacks in wireless ad hoc networks, journal of IEEECommunications Society, ISSN: 0163-6804, vol.46, Issue.4, PP. 127 - 133.

[25] Djahel, S., Nait-Abdesselam, F., Khokhar, A., (2008), An Acknowledgment-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol, ICC '08. IEEE International Conference on Communications, 2008, PP. 2780 - 2785.

[26] Mishra, R., Sharma, S., Agrawal, R., (2010), Vulnerabilities and security for ad-hoc networks, IEEE Conference Networking and Information Technology (ICNIT), PP.192 - 196, 2012.

[27] Kui Ren., Wenjing Lou., Kai Zeng., Moran, P.J., (2007), On Broadcast Authentication in Wireless Sensor Networks, ISSN: 1536-1276, vol.6, Issue.11, PP. 4136 - 4144.

[28] Westhoff, D., Girao, J., Acharya, M., (2006), Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution, and Routing Adaptation, journal of IEEE Computer Society, ISSN: 1536-1233, vol.5, Issue.10, PP. 1417 - 1431.

[29] S.Kumar, G.Pruthi, A.Yadav, M.Singala, (2012), Security Protocols in MANETs, IEEE Conference, PP.530 - 534.

[30] A. Adnane1, R. Tim´oteo, A.Yadav, (2010), Analysis of the implicit trust within the OLSR protocol, DOI: 10.1007/978-0-387-73655-6_6 · Source: OAI, PP.1 - 17.

Author Biography

1st **Bahram Najafpour**, received a B.Sc. in software engineering from University of Zanjan, Iran in (2011) and the M.Sc. degree in software engineering from Iran University of Science and Research (SRBIAU) in (2013). Teaching Computer Courses in universities of Ardabil. His research interests include Wireless Networks, Analysis of computer systems, Software Develop and Image Processing with MATLAB, Rational Rose, NS2, OPNET and have published more than 20 conference and journal papers.