World Wide Journal of Multidisciplinary Research and Development

WWJMRD 2017; 3(7): 68-72
www.wwjmrd.com
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Harpreet Singh
Department of Computer Engineering, Guru Kashi University Talwandi Sabo Bathinda, Punjab, India

Harpal Singh
Department of Computer Engineering, Guru Kashi University Talwandi Sabo Bathinda, Punjab, India

Correspondence:
Harpreet Singh
Department of Computer Engineering, Guru Kashi University, Talwandi Sabo Bathinda, Punjab, India

A Secure and Efficient NETWORK USING OLSR Protocol using Certificate Exchange

Harpreet Singh, Harpal Singh

Abstract
Nodes in MANET are powered by limited batteries and their lifetime is usually less as compared to other networks such as mobile ad hoc networks. In such kind of networks, the nodes must work for longer duration of time because the replacement of the batteries is very costly affair. Since these nodes communicate wirelessly with each other, these nodes are susceptible to various kinds of security attacks. While most of the attacks have the false intention of capturing the packets and information from the network, the malicious nodes tend to drop the packets being routed towards them. These packet dropping attacks result in loss of information while other attacks aim at consuming the resources of the network. It is infrastructure less network. There is no central controller which can control the network performance and secure the network from various kinds of attacks. There requires the special arrangement in the protocol so that the attacker node can be identified and removed. This special arrangement is in the form of certificate exchange. So that two or more persons who has authentic certificate can exchange data amongst themselves. It is the special arrangement where any path which has more packet drop rate will be considered as the path having attacker node. Any new path which has those attacker nodes in the intermediate list will be avoided. So that network performance can be avoided to be downgraded. In proposed technique all the performance parameters like throughput, end to end delay, success rate and packet Delivery ratio has shown the improvement.

Keywords: AODV, OLSR, SAODV.

Introduction
The field of Wireless networks has experienced rapid growth since 1970s. In fact, the combination of radio communications and computer networks were first introduced by the University of Hawaii in 1971 in an experimental network named ALOHANET. This was the first Wireless Local Area Network (WLAN) that offered star topology based bidirectional communications. During the 80s, the technology was drastically improved. At the end of the 90s, wireless networks made great revolution and reached a peak due to the constant growth of the Internet.

Fig. 1 [3]

Mobile Ad-hoc networks (MANETs) have been widely researched during last few years, gathering lots of attention due to rapid increase in mobile devices. Today's world of dynamic changing technology of communication networks, MANETs play a vital role in wireless communication. MANETs are collection of wireless mobile nodes that acts as dynamic

network without use of fix infrastructure and centralized control to authorize other entities in network. MANET comprises of mobile nodes that cooperate with each other using wireless connections to route both data and control packets within the wireless network [1].

Unlike a wired network, nodes in an ad hoc network can free to move in random and arbitrary direction, so frequent changes in topology. These networks are self-configuring network and nodes within MANETs provide a peer-level multi-hopping routing service because each node acts as a router. Also, source to destination communication may require routing information via several intermediate nodes to route a packet to the destination node due to limited transmission range of a node. Each mobile node that communicates with other node via radio wave and can communicate directly to those nodes that is in transmission range of each other. Each participating node in MANETs is independent and makes routing decision like route request, route selection, route update and making new communication link with their neighbor's as well as serving old established [2]. However, all network functions are based on the nodes mutual effort. A simple example of MANETs is shown below.

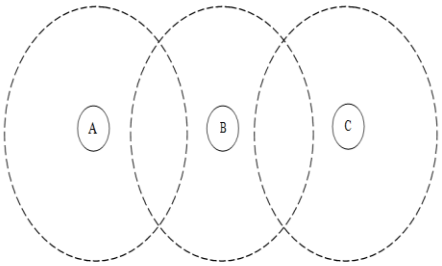


Fig. 2 [2]

In figure, node A wants to communicate to node C. However, node C is not in the direct transmission range of node A. So, node A and C must discover route through node B in order to communicate with each other. However, there is no dependency on infrastructure that makes it robust and low-cost. A MANETs has many benefits, such as and adaptability to highly variable characteristics, namely power, transmission conditions, traffic distribution variations, and load balancing. However, those benefits come with many challenges. New algorithms, protocols have to be designed and developed to create a truly flexible and decentralized network. The system may operate in isolation, or may have gateways to and interface with a fixed network [4].

Related Work

Utpal Kumar Verma et al (2016)**:** In mobile ad hoc networks (MANETs), authentication is a critical issue. It is a tough task to provide security and authentication in MANETs due to the absence of any centralized administration and dynamic topology of the network. It presents a robust and secure mechanism for authentication of nodes in the MANET. The proposed authentication protocol is based on certificate exchange between the nodes. This protocol also uses digital signature with a hash function to maintain the authenticity of certificates [1].

Surendran.S et al. (2015): most MANET routing protocols assume a friendly and cooperative environment, and hence are vulnerable to various attacks. Trust and Reputation would serve as a major solution to these problems. Learning the network characteristics and choosing right routing decisions at right times would be a significant solution. In this work, they have done an extensive survey of fault tolerant protocols and ant colony algorithms applied to routing in MANETs. We propose a QoS constrained fault tolerant ant look-ahead routing algorithm which attempts to identify valid route and look-ahead route pairs which might help in choosing the alternate path in case of valid route failure [2].

G.Narayana et al. (2016): In this paper we have designed an energy efficient polynomial-based group key management protocol for MANET. Thus a self-organized group establishing algorithm is applied in which the Group Manager (GM) is selected based on link quality (LQ) and residual energy (RE). The selected Group manager generates polynomials for intra-group and inter-group communications. Thus each GM includes its current residual energy and link quality information during the broadcast of polynomials. When the link quality or residual energy of GM tends to decrease, the GM is re-elected again by executing the self-organized group establishing algorithm[3].

Jaydip Sen et al. (2015): A *mobile ad hoc network* (MANET) is a collection of mobile nodes that communicate with each other by forming a multi-hop radio network. Security remains a major challenge for these networks due to their features of open medium, dynamically changing topologies, reliance on cooperative algorithms, absence of centralized monitoring points, and lack of clear lines of defense. Design of an efficient and reliable node authentication protocol for such networks is a particularly challenging task since the nodes are battery-driven and resource constrained. This paper presents a robust and efficient key exchange protocol for nodes authentication in a MANET based on multi-path communication. Simulation results demonstrate that the protocol is effective even in presence of large fraction of malicious nodes in the network. Moreover, it has a minimal computation and communication overhead that makes it ideally suitable for MANETs [4].

Algorithm

Step1: A network with different mobile nodes is setup. One node will works as source node and one node will works as destination node.

Step2: Send the route request to the neighbor node for identifying the destination.

Step3 Receive the route replies.

Step4: Send the Certificate from the source nodes to the neighbors which are in the intermediate node list. If intermediate node has higher failure rate then the node will be considered malicious, else it will be declared legitimate.

Step5: Send the data packets on to the route which consists of legitimate nodes.

Step6: Check the network performance under different parameters like Throughput, End to End delay, Packet Delivery Ratio, Success rate.

Step7: Compare the performance on both with and without the attack.

Flowchart for Proposed Algorithm

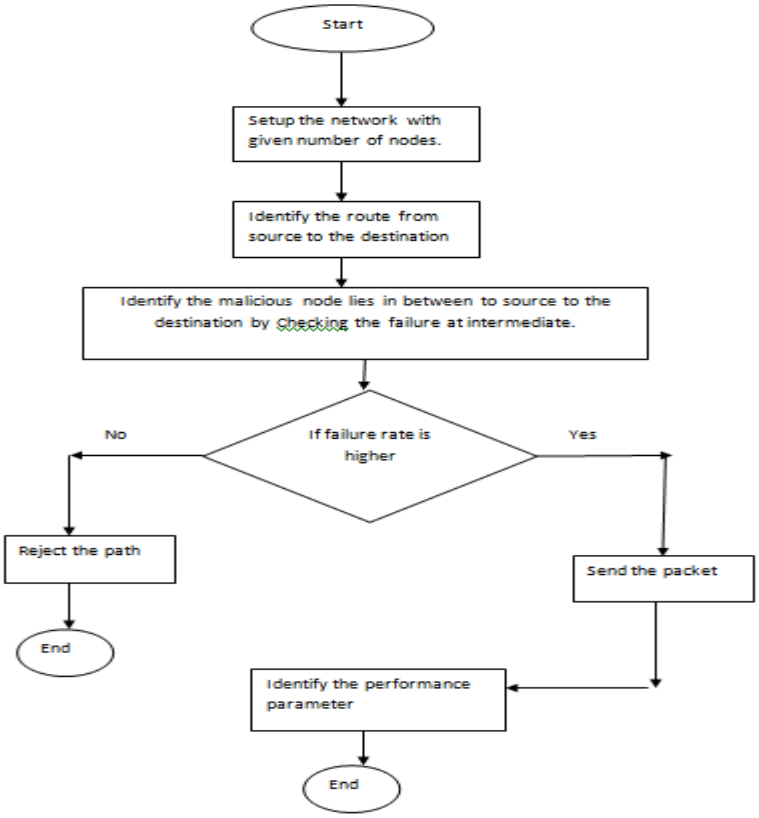


Fig. 3

Results and Discussions

The proposed algorithm is implemented using NS2 2.35 with the following node configuration parameters.

S. No	Parameter Name	Parameter Value
1	Network Size	1100*1100 m^2
2	Max. packet in ifq	500
3	Initial energy (in joules)	50
4	Sleep Power	0.00005
5	TP	0.002
6	TT	0.005
7	IP	1.0
8	Routing Protocol	AODV

Table 1: Node Configuration Parameters

Sample Network 1

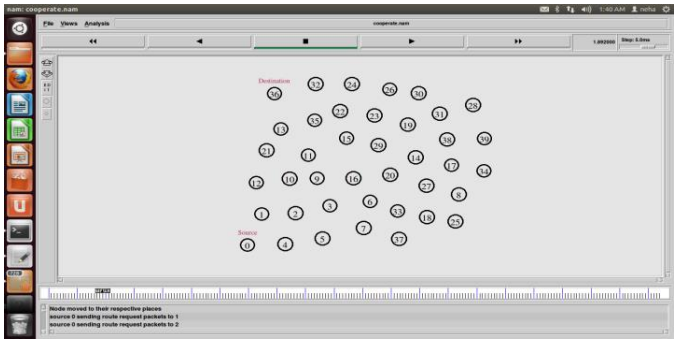


Fig. 4

Nodes are deployed to their respective places. There are total 40 nodes in the network with node number 0 as source node and node number 36 as destination node.

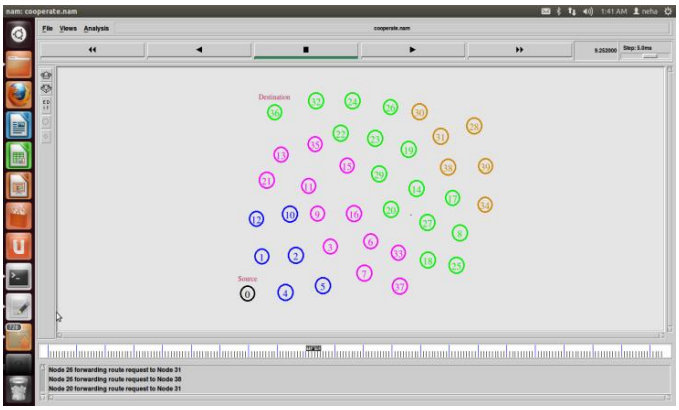
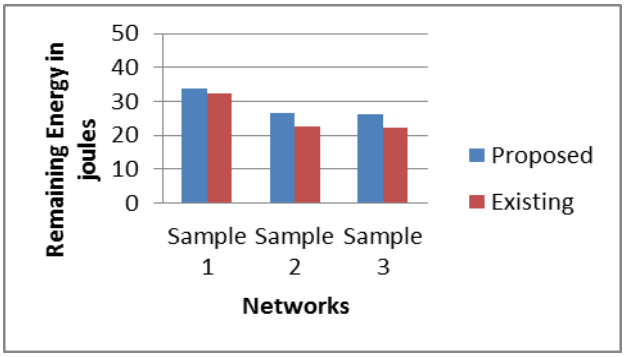
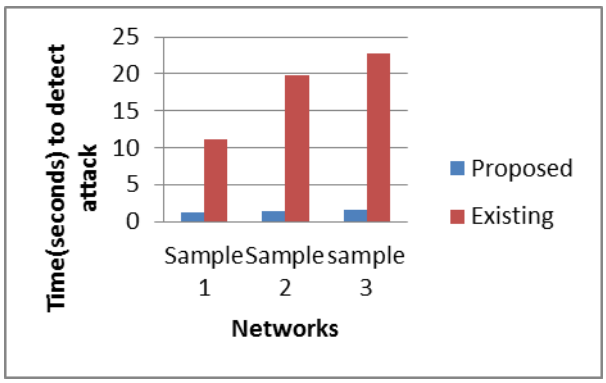


Fig. 5

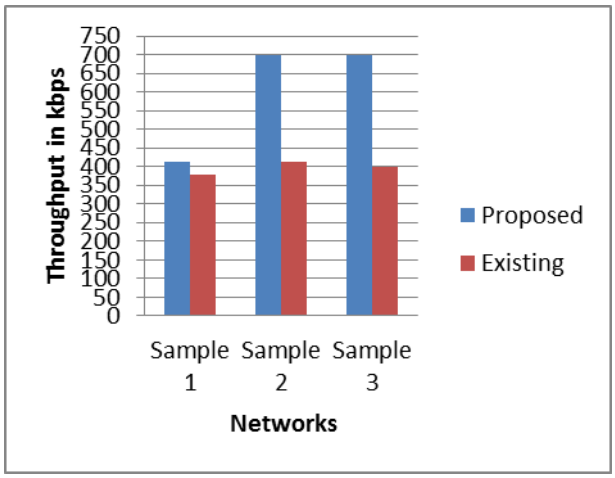
a. Remaining Energy



b. Time Taken to Detect the Attack



c. Throughput



Comparison of Parameters

Comparison of three networks is shown below and in all the cases proposed scheme has outperformed the existing scheme (threshold energy efficient scheme).

Sample Number	Technique	Remaining Energy(J)	Time(sec) to Detect Attack	Throughput(kbps)
1	Proposed	33.75	1.3	412.16
	Existing	32.16	11.1	378.88
2	Proposed	26.57	1.4	698.36
	Existing	22.67	19.8	412.16
3	Proposed	26.11	1.5	698
	Existing	22.26	22.7	398.84

Table 2: Comparison of Parameters

This is due to the fact that whenever the source node obtains the route reply messages, it tends to choose the path having lowest hop count to prevent longer paths and also if any node appears again in path, it will detect that node as attacker node to prevent loops. While on the other hand, the existing scheme relies on comparing the energy of the nodes with the threshold value to defend against such attacks. The existing scheme prevents such attacks after the damage has been done. Thus the existing scheme would tend to utilize more energy than the proposed scheme. The proposed scheme prevents the vampire attack when source node receives route replies, thus this scheme is quick as compared to existing scheme which would detect the attack after its occurrence. So the parameter time taken to detect the attack has shown an improvement over the time taken in the existing scheme. Another parameter namely throughput reflecting the amount of data being received at the destination node has also shown an improvement over the existing scheme

Conclusion and Future Scope

Vampire attacks are considered to be very dreadful attacks for wireless sensor networks since these vampire nodes route the data to destination in iterations and over longer routes. A normal network would have lesser number of nodes from source to destination whereas the paths having the vampire nodes would have considerably more number of nodes. So, the vampire attacks tend to drain out energy of large number of nodes in the network thus causing much harm. The proposed scheme tends to prevent such kinds of attacks in the network thus reducing the wastage of energy. The proposed as well as existing schemes were extensively simulated in NS2.35 and the results were analyzed on the basis of remaining energy, throughput and time taken to detect the attack. The remaining energy in the three networks has showed an improvement of approximately 4.9 percent, 17.20percent and 17.29 percent respectively over the existing scheme, this is attributed to the fact that in proposed scheme AODV protocol would let the source node to wait for five route replies and from these replies select the one having lowest hop countto prevent longer paths and also if any node appears again in path, it will label that node as attacker node to prevent loops. Since routes with vampire nodes have larger hop counts so, by selecting the path with shortest hop count they have been prevented from being chosen to send the data. Whilst on the other hand, the existing scheme relies on comparing the energy of the nodes with the threshold value to defend against such attacks. The existing scheme prevents such attacks after the damage has been done. Thus, the existing scheme would tend to utilize more energy than the proposed scheme. The proposed scheme prevents the attack when the source node receives the route replies, thus it is quick as compared to existing scheme which would detect the attack after its occurrence. So, the parameter time taken to detect the attack has shown an improvement over the time taken in the existing scheme. Another parameter namely throughput reflecting the amount of data being received at the destination node has also shown an improvement of approximately 8.78 percent, 69.43 percent and 75.0 percent respectively in all three networks over the existing scheme. Thus, it can be concluded that the proposed scheme is not only successful in defending against attacks but it is also able to reduce the energy consumption in the network in a robust manner.

There are various cryptographic schemes that exist. This technique can be analyzed against them in future, and it can also be combined with them to make it more secure and work can also be done to find out malicious node that is being responsible for stretch attack.

References

1. Surendran. S, Prakash. S," An ACO Look-Ahead Approach to QOS Enabled Fault- Tolerant Routing in MANETs", august 2015 china.
2. Utpal Kumar Verma,Sushil Kumar, Ditipriya Sinha," A Secure and Efficient Certificate based

Authentication Protocol for Manet", 2016 International Conference on Circuit, Power and Computing Technologies [ICCPCT]
3. G.Narayana1, M.Akkalakshmi2 and A.Damodaram3," Energy Efficient Polynomial Based Group Key Management Protocol for Secure Group Communications in MANET", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 9 (2016) pp 6701-6705
4. Jaydip Sen" A Robust and Efficient Node Authentication Protocol for Mobile Ad Hoc Networks" Innovation Labs, Tata Consultancy Services Ltd. Bengal Intelligent Park, Salt Lake Electronic Complex Kolkata-700091, INDIA
5. Abdul Shabbir & Anasuri Sunil Kumar," An Efficient Authentication Protocol for Security in Mobile Ad Hoc Networks" Special Issue of IJCCT, ISSN (ONLINE) : 2231–0371, ISSN (PRINT) : 0975–7449, Volume- 3, Issue-1
6. Bing Wua, Jie Wua Eduardo B. Fernandez, Mohammad Ilyas,Spyros Magliveras," Secure and efficient key management in mobile ad hoc networks", Journal of Network and Computer Applications 30 (2007) 937–954
7. Abu Taha Zamani, Syed Zubair," Secure and Efficient Key anagement Scheme in MANETs", IOSR Journal of Computer Engineering (IOSR-JCE) p- ISSN: 2278-8727Volume 16, Issue 2, Ver. XI (Mar-Apr. 2014), PP 146-158
8. Katrin Hoeper and Guang Gong," Bootstrapping Security in Mobile Ad Hoc Networks Using Identity-Based Schemes with Key Revocation", Department of Electrical and Computer Engineering University of Waterloo Waterloo, ON, N2L 3G1, Canada.
9. Parmar Amish, V.B.Vaghela," Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol", Procedia Computer Science 79 (2016) 700 – 707
10. Haroun Benkaouha † Abdelkrim Adelli †, Nadjib Badache † Jalel Ben-Othman‡, and Lynda Mokdad," AFDAN: Accurate Failure Detection protocol for MANETs", 978-1-4799-5344-8/15