ROUTING PATH INTRUSION NODE REMOVAL USING OLSR PROTOCOL

J kalidevi[1] | Mrs.A.Wims Magdalene mary[2]
[1](Dept of ECE, PG student, Sri Krishna College of Engineering and Technology, Coimbatore, j.kalidevi@gmail.com)
[2](Dept of ECE, Assistant professor, Sri Krishna College of Engg and Tech, Coimbatore, wimsmary@skcet.ac.in)

Abstract— *The open nature of the suspicious node of the adhoc network leaves it vulnerable to packet loss through link error and packet dropping. The mitigating technique can be used for mounting the packet loss on the wireless adhoc network. Typically, the detection process has been addressed under insider attack cases. Many existing works has carried out to answer these issues but reputation of the system fails due to manipulation of the data. Data integrity plays major problem in the reputation of the system against the data modification attacks. In this paper, we propose an attack resilient technique named as MANET. The MANETs does not have any fixed infrastructure or central access points to the backbone infrastructure to the sensitive information. The OLSR protocol is proactive to the reputation base mechanism to prevent the attacks.*

Keywords— MANET; OLSR Protocol; Packet Hiding; Routing Path

1. INTRODUCTION

The wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless Transmissions, inject spurious messages, or jam legitimate ones. Specifically, the malicious node may evaluate the importance of various packets, and then drop the small amount that is deemed highly critical to the operation of the network. Detecting selective packet-dropping attacks is extremely challenging in a highly dynamic wireless environment. The difficulty comes from the requirement that we need to not only detect the place (or hop) where the packet is dropped, but also identify whether the drop is intentional or unintentional. In this paper, we propose an attack resilient technique named as Packet hiding technique for preventing the denial of service attack through cluster based suspicious node. Data injection can be prevented using cryptographic methods; jamming attacks are much harder to counter. The proposed model extracts the information from routing table about the attacking nature, the similar attacking characteristics nodes are clustered together. The data hiding principle is applied to the normal node clusters in order to achieve the attack free data transmission.

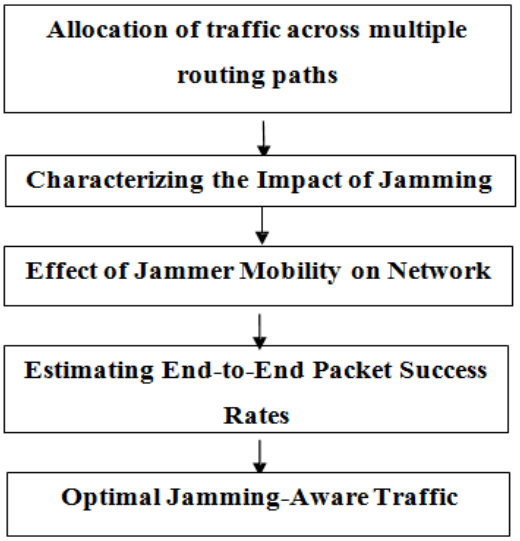
2. LITERATURE REVIEW

IDS system that models the network behavior of data logs across routing table. By monitoring network requests, [1]. we are able to ferret out attacks that independent IDS would not be able to routing operation, using a reverse tracing technique [2]. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again.[3] The CBDS scheme merges the advantage of proactive detection in the initial step and the superiority of reactive response at the subsequent steps in order to reduce the resource wastage.[4] CBDS is DSR (Dynamic Source Routing protocol). [5] As it can identify all the addresses of nodes in the selected routing path from a source to destination after the source has received the RREP message. However, the source [6] node may not necessary be able to identify which of the intermediate nodes has the routing information to the destination or which has the reply RREP message or the malicious node reply forged RREP. identify. Intrusion detection systems have been widely used to detect known attacks by matching misused traffic patterns or signatures [7]. DDoS attacks focus on mitigating malicious bandwidth consumption caused by packets flooding is controlled by big wheel algorithm, as that is the most simple and common method adopted by attackers. The big wheel algorithm works with detection of changes in the address by attacking node [8]. Also, it detects the traffic redundancy and data redundancy in the network the objective of the research work is, to design a system for effective data communication and [9] network management, to find the selfish node, detection time and detection accuracy for each transaction and compare results to determine the performance of selfish node detection. [10] In this section, we describe the implementation of the packet hiding scheme for preserving of the data in the transmission using the following mechanism, [11] It intentionally disturbs the correct behavior of the network. Malicious node can be lying about the status of other nodes, producing a fast diffusion of false negatives or false positives. [12]They can intentionally participate in network communication with the only goal to hide their behavior from the network.[13] The behavior of malicious nodes is modelled from the receiver perspective, which is based on the probability of receiving wrong information about a given node[14] when a contact with a malicious node occurs that is, it receives a[15] Negative about the selfish node, and a Positive about the other nodes.

3. METHODOLOGY

A selfish node usually denies packet forwarding in order to save its own resources. This behavior results in heavy packet loss during the data transmission. Impacts of the

selfish nodes It intentionally disturbs the correct behavior of the network. Malicious node can be lying about the status of other nodes, producing a fast diffusion of false negatives or false positives. They can intentionally participate in network communication with the only goal to hide their behavior from the network. The behavior of malicious nodes is modelled from the receiver perspective, which is based on the probability of receiving wrong information about a given node when a contact with a malicious node occurs that is, it receives a Negative about the selfish node, and a Positive about the other nodes.



3.1 Allocation of traffic across multiple routing paths

In this module we formulate the problem of allocating traffic across multiple routing paths in the presence of jamming as a lossy network flow optimization problem. We map the optimization problem to that of asset allocation using portfolio selection theory which allows individual network nodes to locally characterize the jamming impact and aggregate this information for the source nodes.

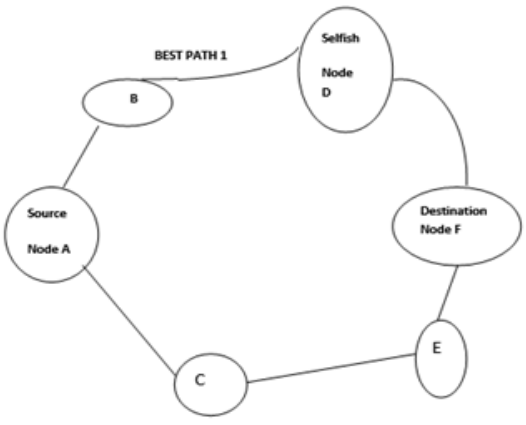


Fig a) Allocation of traffic path

3.2 Characterizing the Impact Of Jamming

In this Module, the network nodes to estimate and characterize the impact of jamming and for a source node to incorporate these estimates into its traffic allocation. In order for a source node s to incorporate the jamming impact in the traffic allocation problem, the effect of jamming on transmissions over each link must be estimated. However, to capture the jammer mobility and the dynamic effects of the jamming attack, the local estimates need to be continually updated.

source node in the network protocol of the new optimized network topology against various routing constraints of the network using routing based on distributed fault handling and energy consuming strategies.

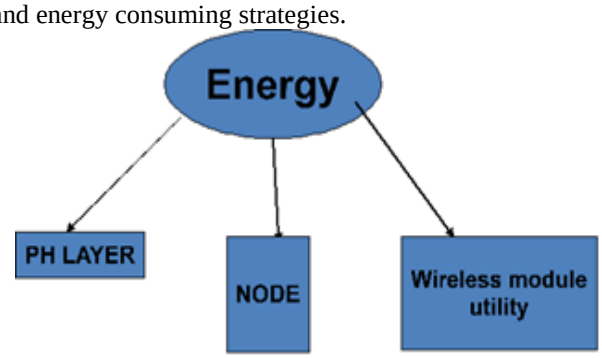


Fig b) Jamming energization layer

3.3 Effect of Jammer Mobility on Network

The capacity indicating the link maximum number of packets per second (pkt/s) eg:200 pkts/s which can be transported over the wireless link. Whenever the source is generating data at a rate of 300 pkts/s to be transmitted at the time jamming to be occurring. Then the throughput rate to be less. If the source node becomes aware of this effect the allocation of traffic can be changed to 150 pkts/s on each of paths thus recovers the jamming path.

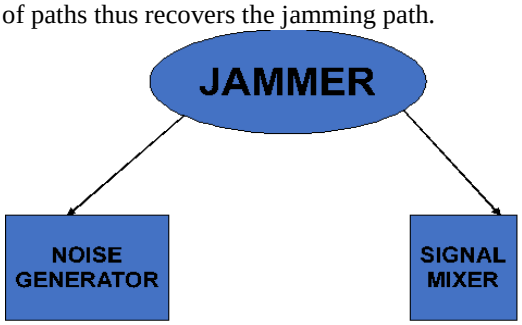


Fig c) Jamming Allocation

the wireless traffic and analyses it to decide whether neighbor nodes are behaving in a selfish manner. When the cluster head detects a selfish node it is marked as a positive detection (or a negative detection, if it is detected as a non-selfish node). The system combines local watchdog detections and the dissemination of this information on the network. If one node has previously detected a selfish node it can transmit this information to other nodes when a contact occurs. This way, nodes have second hand information about the selfish nodes in the network. In general, the analytical evaluation shows a significant reduction of the detection time of selfish nodes with a reduced overhead when comparing cluster model against a traditional watchdog.

3.4 Estimating End-to-End Packet Success Rates

The packet success rate estimates for the links in a routing path, the source needs to estimate the effective end-to-end packet success rate to determine the optimal traffic

allocation. Assuming the total time required to transport packets from each source s to the corresponding destination is negligible compared to the update relay period.

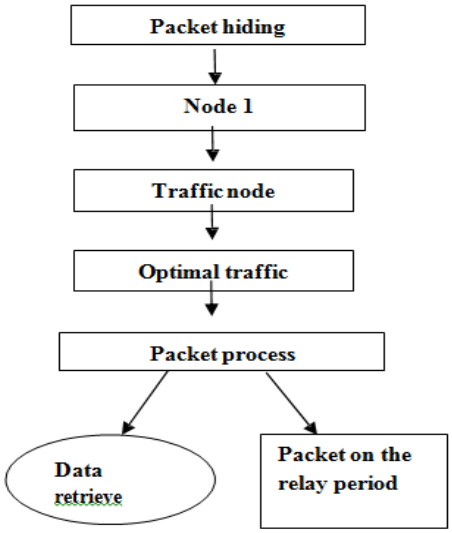


Fig d) Packet flow

1. Consider P as packet with payload and packet header
2. Compute for payload and Packet header size
3. Transform the payload to anonymous content using Homomorphism encryption rules Extract the random text from the payload Transform ()

Text = {text1, Text 2, Text 3,}

Increment each content in text vector by 2 shift hashing process

Cipher text = {hash1, hash2, Hash 3...} Original text ()

If (key==hash key)

Convert the cipher text to original text

Cipher text is incremented by data shift provided by source node.

3.5 Optimal Jamming-Aware Traffic Allocation

An optimization framework for jamming- aware traffic allocation to multiple routing paths for each source node. We develop a set of constraints imposed on traffic allocation solutions and then formulate a utility function for optimal traffic allocation by mapping the problem to that of portfolio selection in finance.

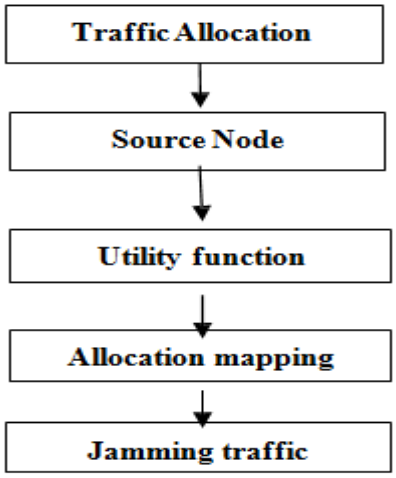


Fig e) Traffic flow

4. CONCLUSION

In this paper, an improved OLSR routing protocol that prevents selection of mobile nodes as MPR nodes is introduced. This proposed method tries to establish more stable and reliable routes in ad-hoc networks. Numerous simulations with different ratio of mobile nodes relative to static nodes are carried out. The simulation results showed that in all of cases, our proposed method decreases PLR of whole network about 15% and decreases PLR of mobile nodes about 10%. The proposed improvement also improves the network overhead by reducing the number of TC messages in the network. The proposed method does not change end-to end packet delivery delay and overall bandwidth of network and increase lifetime of network.

REFERENCES

[1] L. Lazos, S. Liu, and M. Krunz, "Mitigating Control-Channel Jamming Attacks in Multi- Channel Ad Hoc Networks," Proc.Second ACM Conf. Wireless Network Security, pp. 169-180, 2009.

[2] G. Lin and G. Noubir, "On Link Layer Denial of Service in Data Wireless LANs," Wireless Comm. and Mobile Computing, vol. 5, no. 3, pp. 273-284, May 2004.

[3] S. Buchegger and J.-Y.LeBoudee, "Self- policing mobile ad hoc networks by reputation systems," IEEE Commun. Mag., vol. 43, no. 7, pp. 101–107, Jul. 2005.

[4] E. Hern_andez-Orallo, M. D. Serrat, J.-C. Cano, C. M. T. Calafate, and P. Manzoni, "Improving selfish node detection in MANETs using a collaborative watchdog," IEEE Comm. Lett., vol. 16, no. 5,pp. 642–645, May 2012.

[5] Meixing Le, AngelosStavrou, Brent ByungHoon Kang, "Double Guard: Detecting Intrusions in Multitier Web Applications" IEEE Transaction on Department and Secure Computing, Vol 9, No. 4, JULY/AUGUST 2012

[6] R. Rao and G. Kesidis, "Detecting malicious packet dropping using statistically regular traffic patterns in multihop wireless networks that are not bandwidth limited," in Proc. IEEE GLOBECOMConf., 2003, pp. 2957–2961.

[7] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.

[8] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgement- based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2006.

[9] Y. Liu and Y. R. Yang, "Reputation propagation and agreement in mobile ad-hoc networks," in Proc. IEEE WCNC Conf., 2003, pp. 1510–1515.

[10] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable secure routing for ad hoc networks," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 – 9.

[11] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing selfishness in mobile ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2005, pp. 2137–2142.

[12] K. Liu, D. Pramod, K. Varshney, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[13] K. Vishnu and A. J Paul, "Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks," Int. J. Comput. Appl., vol. 1, no. 22, pp. 28–32, 2010.

[14] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.

[15] H. Weerasinghe and H. Fu, "Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation," in Proc. IEEE ICC, 2007, pp. 362– 367.