International Journal Of Advance Research, Ideas And Innovations In Technology

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 6)
Available online at: www.ijariit.com

A novel approach to mitigate the MANET threats using hybrid optimizations

Shabiha Kumari
shabihakumari48@gmail.com
Swami Sarvanand Group of Institutes, Dina Nagar, Punjab

Harjinder Kaur
harrysaini988@gmail.com
Swami Sarvanand Group of Institutes, Dina Nagar, Punjab

ABSTRACT

A MANET is a self-organizing network in which all the sensor nodes of the system are self-governing without any central system to achieve routing. Nodes energetically establish paths to one more to communicate among the nodes, trusting on the neighbor nodes to keep system connected. In this paper the attention is on security matters associated to ad-hoc systems which are mainly required to deliver secure broadcastings and possible security measures to avoid the attacks. Based on the environment of attack, the bouts are categorized into active and passive bouts. So in this paper, the important measure is taken using swarm intelligence approach which will increase the lifetime of the network and decreases the effect of attack in the networks

Keywords— *Ad-Hoc networks, Security threats, Network lifetime*

1. INTRODUCTION

In the previous couple of decades the world has turn into a worldwide town by prudence IT sector. Information Technology (IT) is developing step by step. Organizations have a tendency to utilize more difficult system situations. Regardless of the endeavors of system heads and IT merchants to secure the computing situations, the dangers posed to individual protection, organization security and different resources by attacks upon systems and PCs. The MANETs are unquestionably a piece of this revolution. MANET is an accumulation of wireless devices or hubs that impart by dispatching packets to each other or for another device/hub, without having any framework controlling information for routing. MANET's hubs have boundless network and versatility to different hubs. Having a secured transmission and correspondence in MANETS is a key issue because of the way that there are different sorts of attacks that the mobile system is interested in. To secure correspondence in such systems, understanding the at risk security attacks to MANETs tasks are extraordinary task and concern. MANETs experience is having effects of a mixed bag of security attacks and dangers, for example:

1. Sybil attacks
2. Flooding attack
3. Wormhole attack
4. Black hole attack.

2. APPLICATIONS OF MANETs

Table 1: Areas and the possible scenarios

Areas	Possible scenarios
Military Scenarios	Military communications and automated battle fields mainly based on MANETS network.
Rescue	MANETS helps in Disaster recovery, means additional of fixed infrastructure
Data networks	The exchange of data between mobile devices is also based on MANETS.
Device operations	Wireless connections between various mobile devices are dependent on device networks.
Free internet connection	It also allows us to share the internet with other mobile devices.

In this thesis secure routing mechanism will be done to mitigate the effect of Sybil attack in which multiple copies are produced and affect the whole network in terms of signal losses, path losses, packets delivery and lifetime of the network.

3. SYBIL ATTACKS

It is an unsafe advanced world out there. So the areas must be restricted with some antiviruses to reduce the attack scenarios. Sybil attack deals with the generation of the multiple identities increase the load on the system.

Most systems, similar to a shared system, depend on assumptions of personality, where every PC speaks to one character. A Sybil attack happens when an unreliable PC is captured to claim different characters. Issues emerge when a reputation system, (for example, a record sharing reputation on a system) is deceived into believing that an attacking PC has a disproportionally vast impact. Congruently, the malicious attacker with frequent personalities can exploit them to act malevolently, by either enchanting data or upsetting the data.

4. LITERATURE SURVEY

K.Sumathia et al. [5] presents the achievement of Adaptive HELLO messaging proposal to determine the local link connectivity information for monitor the link status between nodes along with the incorporation of Dynamic on Demand Routing Protocol to decrease the energy consumption of mobile nodes to certain extent. Ahmed, Mariwan et al. [6] they are suggesting modification in conventional AODV protocol to prevent Sybil attack. The essential idea to detect and isolate spiteful nodes is which the use of false messages. Jhaveri, Rutvij et al. [7] proposed a scheme for Ad-hoc On-demand Distance Vector protocol, in which an middle node detects the spiteful node sending false routing in sequence; routing packets are used not only to pass routing in sequence, but also to pass information about spiteful nodes. V. Kamatchi et al. [8] deals with prevention of both types of sybil attacks and secure data communication using secret sharing and Random Multipath Routing Techniques.

5. RESULTS AND DISCUSSIONS

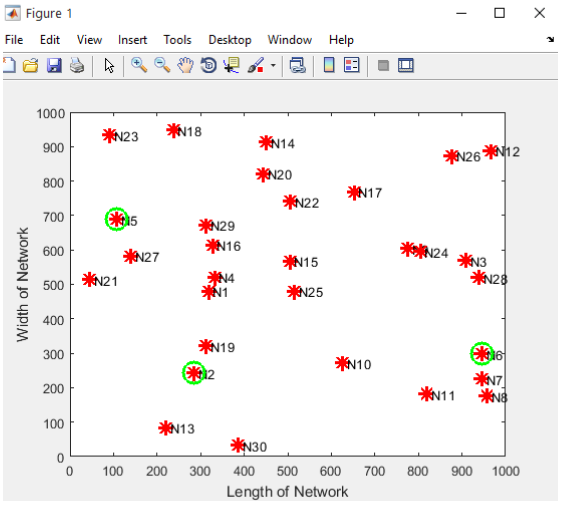

Fig. 1: Sensor Network

The figure 1 shows the network creation using nodes deployment and shows the nodes are deployed in the random fashion. The normal nodes are red in color and the nodes which are green in color are the nodes having energy higher than the original nodes in the network

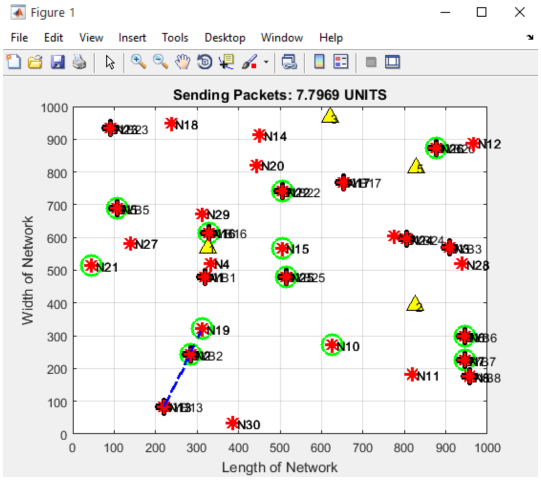

Fig. 2: Routing process

The figure 2 shows the routing between the nodes and the Sybil node attack which are yellow in color and considered as the malicious nodes in the network. The nodes are the neighbor nodes which are participating in the routing process in the presence of the attack. The network area is taken in 1000 meters in length and 1000 meters in width.

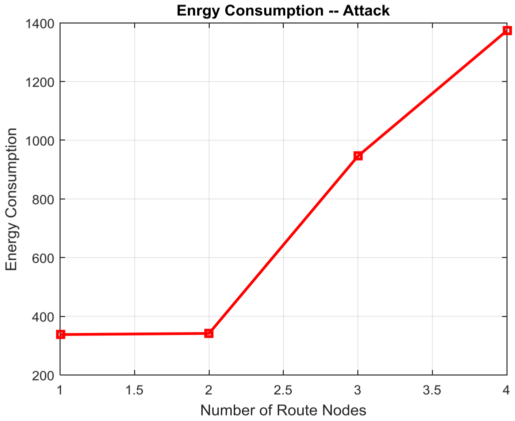

Fig. 3: Energy Consumption

The figure 3 shows the energy consumption in the presence of sybil attack and shows that the system is having high consumption of energy with increase of the sybil nodes which is 1400 mJ.

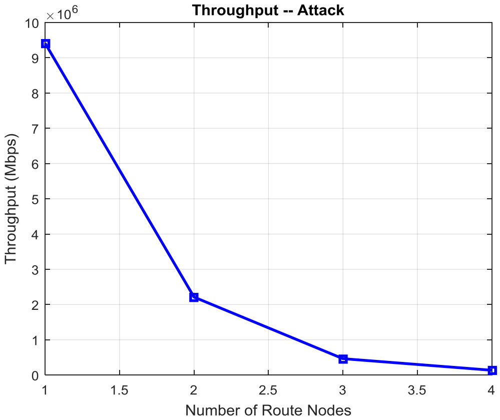

Fig. 4: Throughput (%) with Sybil attack

The figure 4 shows the throughput in terms of packet deliveries which is decreasing and are evaluated with respect to the Sybil attack which shows that the system is degraded in terms of overall performance of the system.

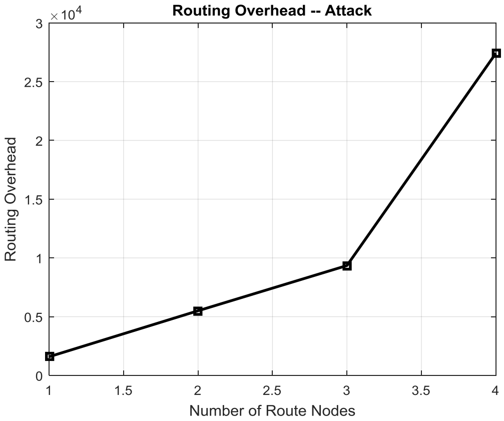

Fig. 5: Routing Overhead

The above figure shows the routing overhead of the network in the presence of the Sybil attack and is very high which increases the congestion in the network.

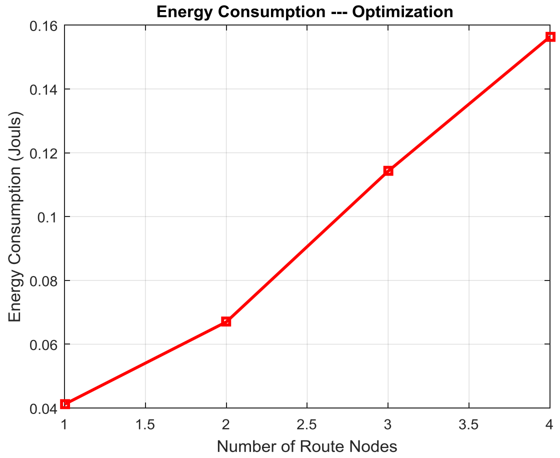

Fig. 6: Energy consumption (Optimization)

The figure 6 shows the energy consumption using hybrid swarm optimization and shows the proposed approach is able to achieve less energy consumption than the attacked consumption in the presence of Sybil attack which shows the robustness of the system.

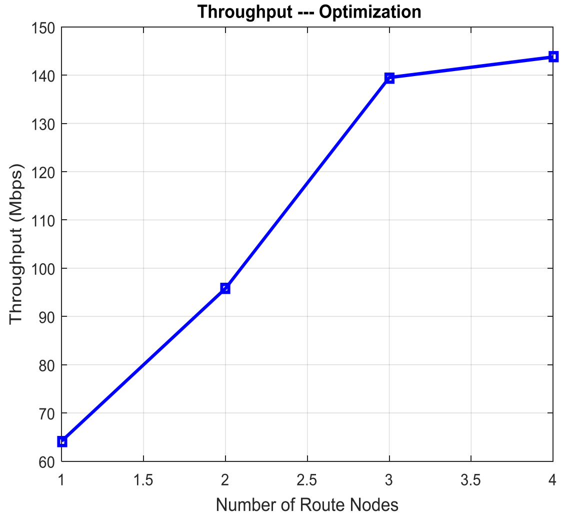

Fig. 7: Throughput with optimization

The figure 7 shows the throughput using optimization and shows that our proposed swarm intelligence approach is able to achieve high packet deliveries which results in high throughput and increases the lifespan of the network. If the throughput is high then the more packets are successfully delivered to the base station.

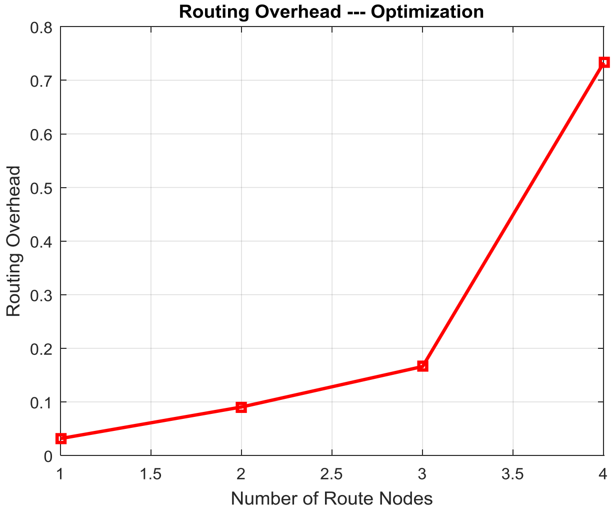

Fig. 8: Routing overhead with optimization

The above figure shows the routing overhead in terms of congestion of the networks and shows that the proposed approach is able to achieve low routing overhead for high packet deliveries to increase the lifespan of the network

Table 2: Performance comparison

Parameters	Base	Proposed
Throughput	97%	98.5%

6. CONCLUSION AND FUTURE SCOPE

MANET is used in various types of real time application like military, pollution control or any type of wireless detection arrangements etc. Therefore the security, delay & Protection becomes main task in Ad-hoc networks. This paper deals with the mitigation and reduction of the effect in high dense MANET systems. So the swarm intelligence approach is able to achieve high reduction of effect and maintain the routing of the nodes in optimized manner and increase the lifespan of the network. Security confrontations must be robust adequate to avoid contender to disturb the schemes. It is compulsory to handle the information with full confidentiality & with amazing level of security. The Future work can be the trust management schemes to provide more security and less error rate probabilities which more increase the lifespan of the network.

7. REFERENCES

[1] Baldini, Gianmarco, Vincent Mahieu, Igor Nai Fovino, Alberto Trombetta, and Marco Taddeo. "Identity-based security systems for vehicular ad-hoc networks." In Connected Vehicles and Expo (ICCVE), 2013 International Conference on, pp. 672-678. IEEE, 2013.
[2] Taneja, Sunil, and Ashwani Kush. "Energy efficient, secure and stable routing protocol for MANET." Global journal of computer science and technology 12, no. 10-E (2012).
[3] Sharma, Nidhi, and Alok Sharma. "The black-hole node attack in MANET." In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, pp. 546-550. IEEE, 2012.
[4] Sogani, Priyanka, and Dr Aman Jain. "A Study on Security Issues in Mobile Ad Hoc Networks." IJIACS ISSN (2015): 2347-8616.
[5] Koul, Ajay, and Mamta Sharma. "Cumulative Techniques for Overcoming Security Threats in Manets." International Journal of Computer Network and Information Security 7, no. 5 (2015): 61.
[6] Nithya, S., S. Prema, and G. Sindhu. "Security Issues & Challenging Attributes in Mobile Ad-Hoc Networks (MANET)." (2016).
[7] Shabbir, Asif, Fayyaz Khalid, Syed Muqsit Shaheed, Jalil Abbas, and M. Zia-Ul-Haq. "Security: A Core Issue in Mobile Ad hoc Networks." Journal of Computer and Communications 3, no. 12 (2015): 41.
[8] Jen, Shang-Ming, Chi-Sung Laih, and Wen-Chung Kuo. "A hop-count analysis scheme for avoiding wormhole attacks in MANET." Sensors 9, no. 6 (2009): 5022-5039.
[9] Mishra, Balmukund, and Yashwant Singh. "An approach toward the optimization of witness based node clone attack." In Image Information Processing (ICIIP), 2015 Third International Conference on, pp. 506-510. IEEE, 2015.
[10] Chacko, Namrata Marium, Shini Sam, and P. Getzi Jeba Leelipushpam. "A survey on various privacy and security features adopted in MANETs routing Protocol." In Automation, Computing, Communication, Control and

Compressed Sensing (iMac4s), 2013 International Multi-Conference on, pp. 508-513. IEEE, 2013.

[11] Hinds, Alex, Stelios Sotiriadis, Nik Bessis, and Nick Antonopoulos. "Performance Evaluation of Security Algorithms for the AODV MANET Routing Protocol." In Emerging Intelligent Data and Web Technologies (EIDWT), 2012 Third International Conference on, pp. 311-315. IEEE, 2012.

[12] Satheesh, N., and K. Prasadh. "Analysis and Parameterized Evaluation of Impact of Wormhole Attack Using AODV Protocol in MANET.International Journal 3, no. 9 (2013).