RESEARCH ARTICLE OPEN ACCESS

Prevention of Sybil Attacks in VANETS Using Bacterial Foraging Optimizations Algorithm

Sakshi Gupta [1], Taranjit Singh Aulakh [2]
Research Scholar [1], Assistant Professor [2]
Departmen of Coputer Science and Engineering
Bgiet, Sangrur
Punjab - India

ABSTRACT
The military tactical and other security-sensitive operations are still the main applications of ad hoc networks, although there is a trend to adopt ad hoc networks for commercial uses due to their unique properties. However, similar to other networks, VANET also vulnerable to many security attacks. VANET not only inherits all the security threats faced in both wired and wireless networks, but it also introduces security attacks unique to itself. Among various attacks, Sybil attack is most crucial attack in network. In this paper, we recommend a privacy-preserving system in the direction of detecting Sybil attacks in VANETs under a commonly utilized framework in the existing work. The framework assumes that vehicles communicate with each other in a multi-hop manner.in this we have utilized bacteria foraging optimization algorithm to optimize the network nodes. The results are being evaluated on the basis of parameters such as throughput, energy consumption, error rate, and end to end delay. The whole stimulation model takes place in MATLAB 7.10 environment.

Keywords:- VANET, Security, Bacteria Foraging Optimizations Algorithm, Sybil attack

I. INTRODUCTION TO VANET

VANETs stands for Vehicular Ad-hoc Networks. A vehicular ad-hoc network is a self-configuring network of wireless links connecting mobile nodes. These nodes may be routers and/or hosts. The mobile nodes communicate directly with each other and without the aid of access points, and therefore have no fixed infrastructure. They form an arbitrary topology, where the routers are free to move randomly and arrange themselves as required. Each node or mobile device is equipped with a transmitter and receiver. They are said to be purpose-specific, autonomous and dynamic. This compares greatly with fixed wireless networks, as there is no master slave relationship that exists in a mobile vehicular ad-hoc network.

Conventionally in Ad hoc Networks and Sensor Networks, three categories of defense in contradiction of Sybil assaults are acquaint with, together with: identity registration, radio resource testing, as well as position verification [1]. Radio resource testing is dependent upon the supposition in which a radio cannot direct or receive concurrently on more than one channel. Identity cataloguing alone could not preclude Sybil assaults, for the reason that a malevolent node might acquire several identities through some non-technical approaches such as stealing. Additionally, strict cataloguing became reason for serious privacy anxieties. In position certification, the network authenticates the position of every single node and this also guarantees that every particular physical node is bound with only single identity. An amount of position (or distance) verification methods [3, 4, 5, and 6] have been projected lately. Sybil assaults are fairly dangerous intended for a variability of network applications. Hard work have been done in the direction of perceiving Sybil nodes in MANETs and Sensor Networks.

In this paper, we recommend a privacy-preserving system in the direction of detecting Sybil attacks in VANETs. This framework assumes that vehicles communicate with each other in a multi-hop manner. In this we have utilized BFO algorithm to optimize the network nodes. The results are being evaluated on

the basis of parameters such as throughput, energy consumption, error rate, and end to end delay.

II. SYBIL ATTACK IN VANET

A Sybil attack consists of an adversary assuming multiple identities to defeat the trust of an existing reputation system. When Sybil attacks are launched in vehicular networks, the mobility of vehicles increases the difficulty of identifying the malicious vehicle location. A Sybil attack is one in which a malicious node on a network illegitimately claims to be several different nodes simultaneously. It allows malicious sender to create multiple fake identities (called Sybil nodes) to act as normal nodes .It is an attack wherein a reputation system is subverted by forging identities in peer-to-peer networks.

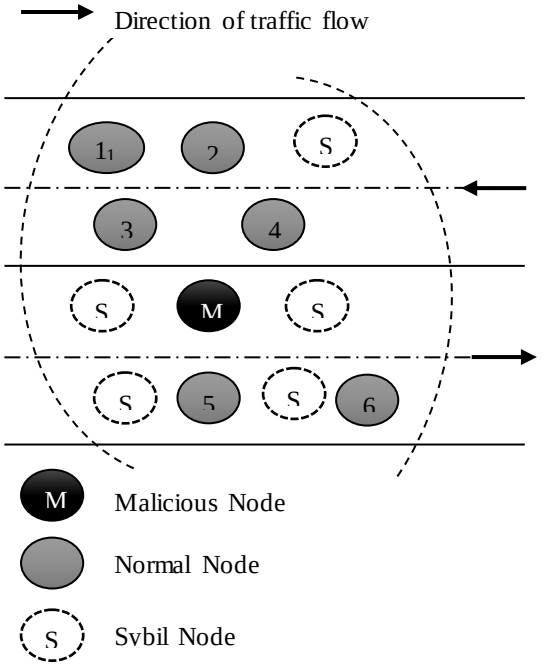

Fig.1 An example VANET under Sybil attacks.

It is an unsafe advanced world out there. Security and antivirus programming is essential for any system. Restricted security can separate is in a Sybil attack. False information reported by a single malicious vehicle may not be sufficiently convincing. Applications may require several vehicles to reinforce a particular information, before accepting it as truth. However, a serious problem arises when a malicious vehicle is able to pretend as multiple vehicles called a Sybil attack, and suitably reinforce false data. If benign entities are unable to recognize a Sybil attack [7], they will believe the false information, and base their decisions on it. Hence, addressing this problem is crucial to practical vehicular network systems. Sybil attack is a kind of security risk when a hub in a system guarantees various characters.

III. BACTERIA FORAGING OPTIMISATION ALGORITHM

Passino [2] discovered this new technique. It is technique of the nature inspired optimization algorithm. In this the bacteria search for nutrients in order to maximize the energy per unit time. When bacteria search for food, then the movement is done with the set of tensile flagella. Flagella is the threadlike structure that enables many bacteria to move from one place to another .Flagella has two basic operations. When the flagella of the bacteria are revolved in the right-handed direction, each flagellum stretches the cell. Each flagella moves independently. This algorithm mainly consists of following steps:

Chemotaxis This process imitates the movement of bacteria via swimming and tumbling. Sometimes, it can swim for a period of time in same direction or it may tumble. With counter clockwise direction, bacterium moves in the straight line. With clockwise, the flagellum moves in different direction.

Swarming The cells when gets energetic with the high level of succinate release aspartate, which helps them to get aggregate into groups and density of the bacteria increases.

Reproduction The bacteria with low level of nutrients, least healthy bacteria will die while the bacteria with the good health will split into two bacteria.

Elimination and Dispersal Sometimes there is the sudden change in the environment due to various reasons like raise in temperature. This may kill the group of bacteria that are currently in that part which is rich in nutrients. Elimination and dispersal have the impact of destroying chemotactic progress.

IV. PROPOSED MODEL

The simulations were carried out by using MATLAB as the language that we use to develop the proposed framework. Below, we have given the methodology followed by the proposed framework flow chart. The methodology of the proposed work is given in steps below:

Step 1: Start

Step 2: Initialize with entering number of network vehicle nodes to configure.

Step 3: Then, we search Sybil nodes in the cache memory of the network. A graph will appear showing the X and Y coordinate.

Step 4: Once, Sybil nodes are found in several rounds. Then, evaluate parameters in Sybil attack such as energy consumption , throughput, end to end delay and error rate.

Step 5: After evaluation with Sybil attack in the network, we apply Bacteria Foraging Optimisation Algorithm on the network utilizing Fitness function for optimization purpose.

Step 6: Then, we evaluate parameters again on the same network after applying Bacteria Foraging Optimisation Algorithm on parameters like energy consumption, throughput, end to end delay and error rate.

Step 7: The result is obtained.

V. RESULTS

5.1Computation Parameters

a) Throughput: Throughput is the number of packets sent or messages delivered over the network in given time.
b) End to End delay: End to End Delay signifies the total amount of time taken by a packet from source to destination.
c) Error rate: the error rate is the number of bits having errors to the total number of bits received in a transmission from source to destination.
d) Energy Consumption: Energy consumption is the energy consumed by packets to deliver the packets from source to destination.

Implementations

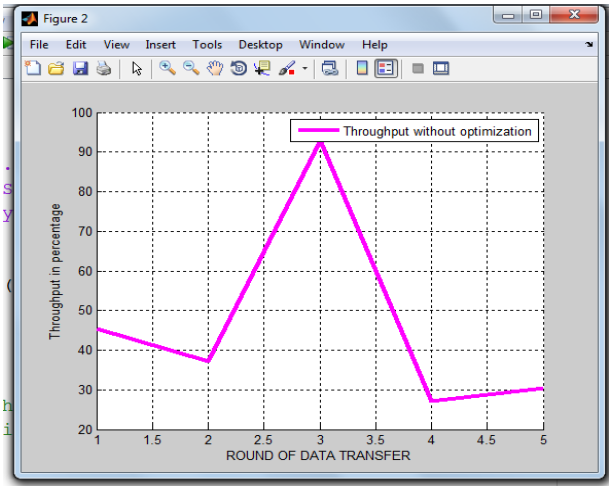

Fig.2 Throughput without optimization

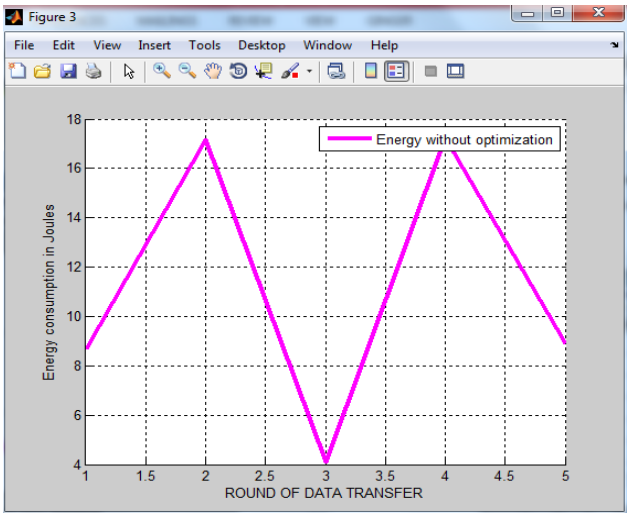

Fig.3 Energy consumed without optimization

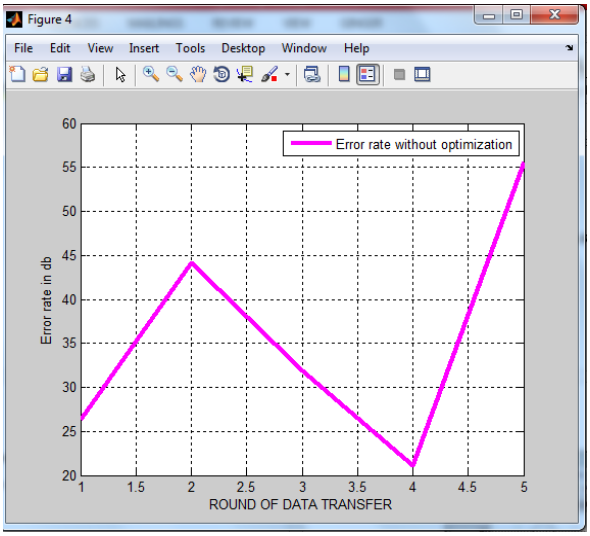

Fig.4 Error Rate without optimization

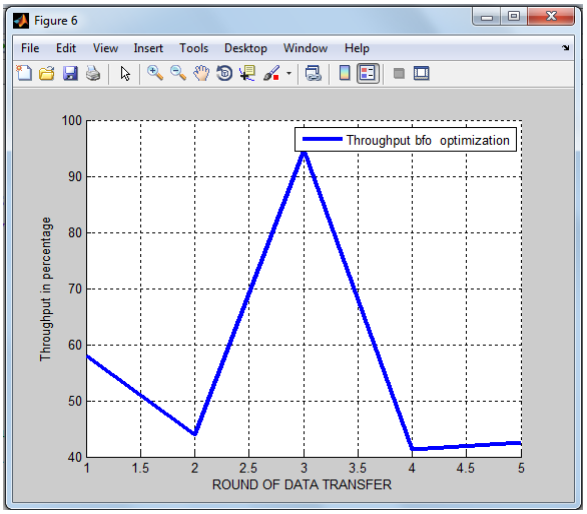

Fig.6 Throughput with optimization

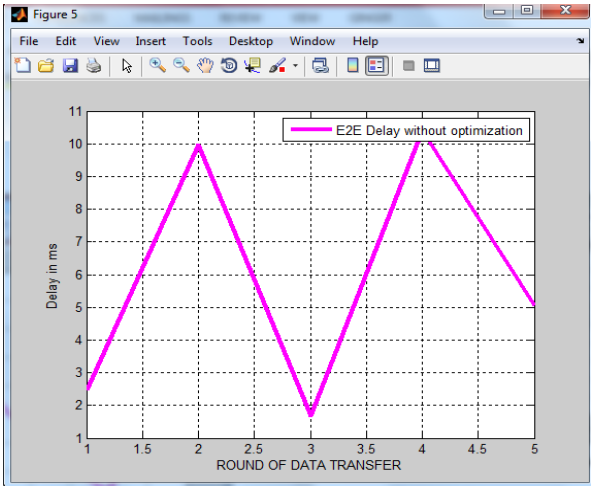

Fig.5 End to End Delay without optimization

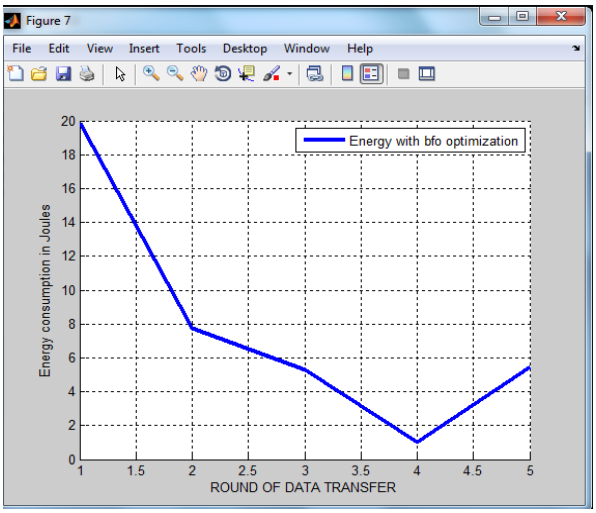

Fig.7 Energy consumption with optimization

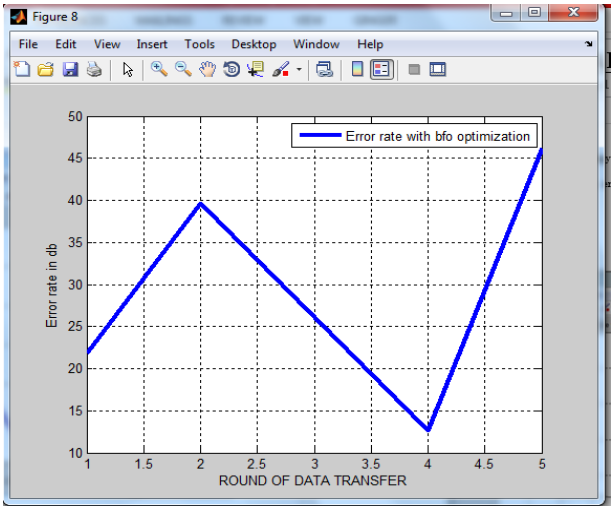

Fig.8 Error Rate with optimization

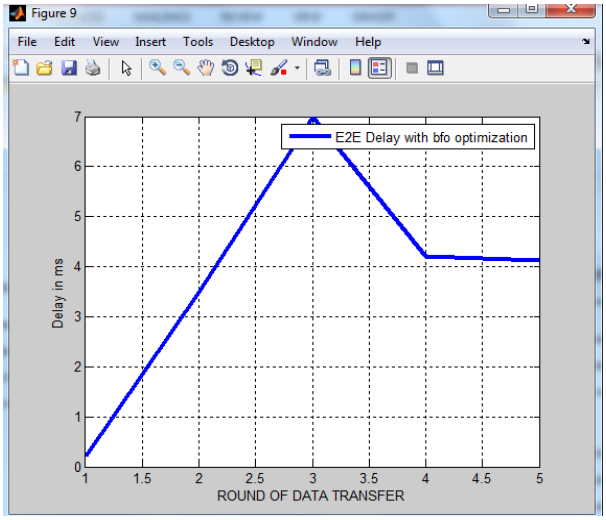

Fig.9 End to End Delay with optimization

VI. CONCLUSION& FUTURE SCOPE

In this paper, the issues related to security like Sybil attack has been reviewed. Then an Intrusion Detection System (IDS) especially for Sybil attacks is implemented using BFO Algorithm, and then tested with networks of varied node configurations in VANET architecture. The algorithm is tested for 20 nodes and the performance analysis is done in terms of throughput, BER, Energy consumption and end to end delay. In the end BFO optimization parameters are compared with without optimization parameters. And it is concluded that Sybil attack prevention is achieved at greater rate when BFO has been used.

Future scope lies in the use of the hybridisation of BFO algorithm with other routing protocols like AODV or DSDV. As they are also vulnerable to this type of attacks.

REFERENCES

[1] P. Golle, D. Greene, J. Staddon, *Detecting and correcting malicious data in VANETs*, in: Proc. of ACM International Workshop on Vehicular ad Hoc Networks, VANET 2004, pp. 29–37, 2004.

[2] Kevin M. Passino, "Bacterial Foraging Optimization", International Journal of Swarm Intelligence Research", March 2010

[3] S. Brands, D. Chaum, *Distance-bounding protocols*, in: Proc. of Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, Springer-Verlag, Inc., 1994, pp. 344–359.

[4] P. Bahl, V.N. Padmanabhan, RADAR: *an in building rf-based user location and tracking system*, in: Proc. of IEEE Infocom 2000, pp. 775–784, 2000.

[5] N. Sastry, U. Shankar, D. Wagner, *Secure verification of location claims*, in: Proc. of the 2003 ACM Workshop on Wireless Security, WiSe 2003, pp. 1–10, 2003.

[6] S. Capkun, J.-P. Hubaux, *Secure positioning of wireless devices with application to sensor networks*, in: Proc. of Infocom 2005, pp. 1917–1928, 2005.

[7] Scott M.Thede, "*An Introduction to Genetic Algorithm*" IN 46135, JCSC 20, 1 (October 2004).[7]

[8] Ali Akbar Pouyan, Mahdiyeh Alimohammadi, "*Sybil Attack Detection in Vehicular Networks*", Computer Science and Information Technology 2(4): 197-202, 2014.

[9] Harsimrat. *"Efficient Detection & Prevention of Sybil Attack in VANET"*,IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 9, September 2015.