Research Journal of Applied Sciences, Engineering and Technology 10(3): 344-349, 2015
DOI: 10.19026/rjaset.10.2497
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: December 29, 2014 Accepted: February 8, 2015 Published: May 30, 2015

Research Article

Enhancing the Performance Metrics by Using Genetic Algorithm

A. Gayathri and P. Narayanasamy
Department of Information Science and Technology, Anna University, Chennai-24, Tamil Nadu, India

Abstract: Security is a vital factor in the field of MANETS. Many researchers are fascinated in finding solution for security. To make it secure EAACK with watchdog mechanism is used, although these techniques avoid intrusion over the network, it also reduces the performance metrics of the network by delay in energy and packet delivery ratio. EAACK is composed of three parts namely ACK, S-ACK and MRA. Hence, we use efficient and secure cryptographic technique with the help of combining EAACK with Genetic Algorithm is used. By using this technique the performance metrics is enhanced and the network performance is achieved successfully. Here we have obtained results from NS2 simulation.

Keywords: Cryptography, EAACK, genetic algorithm, MANET, security, watchdog

INTRODUCTION

Security plays a tremendous role in the field of MANET. Moreover it has various challenges to be faced in its perspective. As MANET has a wide space in the field of research, many new techniques come into the role of challenge. Moreover MANET has characteristics such as dynamic state, infrastructure less, bandwidth-constrained, energy constrained operations and lack of physical security (Shakshuki *et al*., 2013). Due to dynamic nature of MANET, security is an important aspect in the network communication. In order to protect the network from intruders, there exist various techniques. Among them security is a vital factor to guard the network from attacks. Security can be given in two aspects such as prevention and detection.

Intrusion is defined as, any disturbance found in the normal activity of the network. Intrusion prevention technique is the first line of defense that is used to reduce intrusions in the network, when intrusion happens in the network it cannot be guarded spontaneously. There are various methodologies which are used in intrusion detection to detect the malicious activities in the network (Owais *et al*., 2008). Such techniques used to detect the malicious activity are categorized into two divisions namely signature based detection and anomaly based detection.

An anomaly detection method uses a baseline profile of normal activity of a network or abnormal activity of a network. Any network that deviates from the normal activity is said to be an anomaly. The main drawbacks of these techniques are having high false alarm rate and unable to identify the type of attack. The importance of using anomaly method is the ability to detect the new type of attack and that make it efficient for MANET (Barani, 2014).

By using Intrusion detection technique in MANET to avoid the vulnerability caused by an attack. Hence we use efficient cryptographic techniques to guard the network from attackers/intruders. By using G-EAACK, the performance of the network is increased.

MATERIALS

Watchdog method: Many IDS in MANETS is based on extension of Watchdog concept. The main issues involved in Watchdog is:

- Ambiguous collusions
- Receiver Collisions
- Limited transmission power
- False misbehavior report
- Collusion
- Partial dropping

TWOACK: This concept was proposed by Liu *et al*. (2007). The main task of TWOACK is to solve the unsolved issues involved in watchdog. The TWOACK solves two issues of watchdog mainly:

- Receiver collusion
- Limited transmission power (Biradar and Thool, 2013)

TWOACK uses DSR protocol: The working process of TWOACK is explained as follows, it consists of

Corresponding Author: A. Gayathri, Department of Information Science and Technology, Anna University, Chennai-24, Tamil Nadu, India

three nodes namely node 'A', node 'B' and node 'C'. The node 'A' forwards data packet 'P1' from node 'A' to node 'C' through node 'B' to have two hop count. If node 'A' receives the acknowledgement packet from node 'C', then it is successful. If not, it is treated as malicious node. This process is repeated until all nodes are participated in the transmission. Moreover TWOACK detects the misbehaving links by acknowledging the data packet from the source to the destination. This EAACK consists of three parts namely ACK, S-ACK and MRA (Shakshuki *et al*., 2013).

ACK: In general, ACK is known as end-to-end acknowledgment scheme. ACK works for EAACK, in order to reduce network overhead. In the ACK mode, node 'S' forwards ACK data packet 'P1' to the destination node 'D'. If all the nodes in route are cooperative then node 'D' successfully receives the acknowledgment packet 'P1' in the same route in the reverse order. Within the time period, if the node 'S' receives 'P1', then it is stated as packet transmission is successful between node 'S' to node 'D'. Or else, node 'S' will move to next mode known as S-ACK mode.

S-ACK: Liu *et al*. (2007) proposed S-ACK scheme. It is an improved version of TWOACK scheme, The S-ACK scheme is mainly used to detect the misbehaving nodes in the route, S-ACK scheme is described as follows; it consists of three consecutive nodes which function together to find the misbehaving nodes, In each node there will be three consecutive nodes in the route, the third node is used to send S-ACK packet to the first node. The role of using S-ACK mode is to find the misbehaving nodes in the presence of receiver collision or limited transmission power.

The working principle of S-ACK mode is as follows, each three consecutive nodes work in a group to detect misbehaving node in the network. Node F1 sends S-ACK data packet to F2. Node F2 forwards data packet to F3. This Node F3 has to send acknowledgment packet to node F2. Then F2 forwards the acknowledgement packet to F1. If F1 receives the acknowledgement packet within the time period, then it will be stated as successful or else misbehavior report is generated for F2 and F3. In order to confirm the misbehavior report, source node switch to MRA mode and confirm this misbehavior report. This is an important step to detect false misbehavior report in our proposed scheme.

MRA: The basic concept of MRA method is to detect the misbehaving nodes in the presence of false misbehavior report. This false misbehavior report is generated by malicious attackers in order to generate the true node as malicious. The main function of MRA scheme is to check whether the destination node receives the missing packet through an alternate route. The working principle of MRA scheme is as follows, at first the source node searches its local database to find the alternate route to reach the destination node. If the route have not found, it starts using DSR to find the destination route. Due to dynamic nature of MANET, it is open to find multiple routes between two nodes. When the destination node receives a packet, it searches from its local knowledge-base and compares whether the packet was already received. If the packet was received already then it is declared as a malicious node, Or else the packet received is accepted and trusted. The importance of using this MRA scheme is to identify the malicious node in the presence of false misbehavior report as said earlier (Liu *et al*., 2007).

METHODOLOGY

Working methodology of the proposed method: The main idea of the proposed technique is framed into four steps, namely:

- Using of EAACK method
- Where EAACK method consists of ACK, S-ACK and MRA
- With this EAACK method, the genetic algorithm concept is incorporated
- The resultant of this method yields a better performance than EAACK method

Genetic algorithm: The Concept of Genetic algorithm was introduced by John Holland. This GA concept was taken from natural evolution.
Natural evolution has the following features:

- The individual characters are encoded in the chromosome.
- Each chromosome has its own fitness with respect to the environment it exists.
- The resultant chromosomes are judged effectively in order to survive and produce next generations of powerful individuals.

It is based on tracking the neighbor nodes behavior history and its fitness function. It is having three steps working in which fitness function calculation is important to find the misbehaving nodes and also increase the QOS performance than EAACK with digital signature.

Node history: A network consists of set of nodes and here the collection of nodes is called network. Each node consists of node history, based upon the node history; it is directed to routing process.

Node behavior: At first each node is identified as trusted node based upon the behavior in the network.

Work flow of genetic algorithm: Figure 1 explains the basic workflow process of the proposed technique:

Fig. 1: Work flow of genetic algorithm

- To initialize, the generation is set as zero
- Initialize the population
- As per population it will perform the fitness of individual nodes and arrange it in order,
- Range the individuals according to the fitness of individuals
- Then perform crossover and mutation
- Followed that, perform the fitness value
- There after the resultant is arranged according to the order
- Maintain the pop size individuals that contain fitness
- Finally the performance metrics are measured

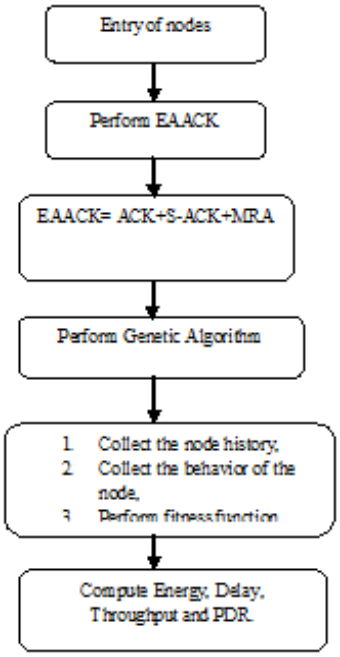

Fig. 2: Proposed G-EAACK flow

Workflow of the proposed method: Figure 2 shows the proposed method of G-EAACK process in detail. The nodes in the network is performed with EAACK. EAACK consists of ACK, S-ACK and MRA. The output of EAACK is performed with genetic algorithm. In this concept, the output of EAACK is treated with genetic algorithm. This Genetic Algorithm consists of three steps of process, at first collect the node history, then node behavior and finally performs fitness function. The output is rated by its performance metrics.

DISCUSSION

Performance metrics: The different parameters used to compare the performance are described below:

- The performance of genetic algorithm is based on Energy, delay, throughput and packet delivery ratio.

Packet delivery ratio: In Fig. 3 it is defined as the number of packet sent by the application which is received by the receiver.

Energy: In Fig. 4, it is defined as the amount of energy spent during the transmission of packet from source to destination.

Delay: In Fig. 5, delay is defined as the time spent to deliver the data packets from the source to the destination.

Fig. 3: Packet delivery ratio graph

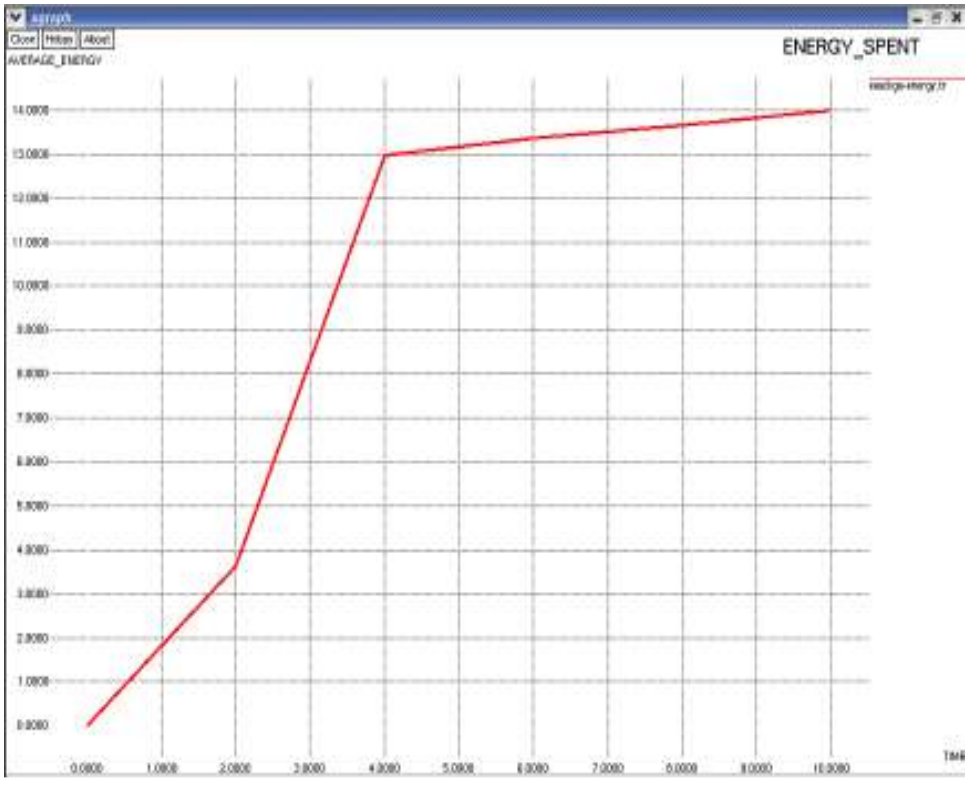

Fig. 4: Energy graph

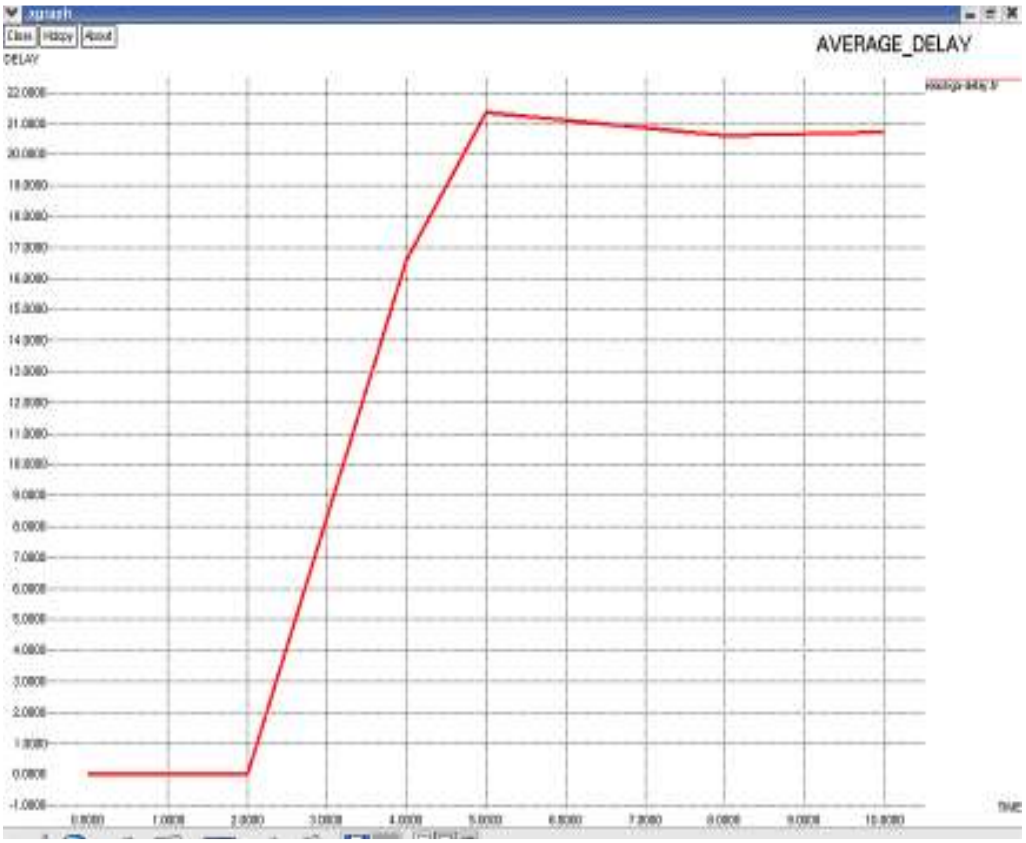

Fig. 5: Delay graph

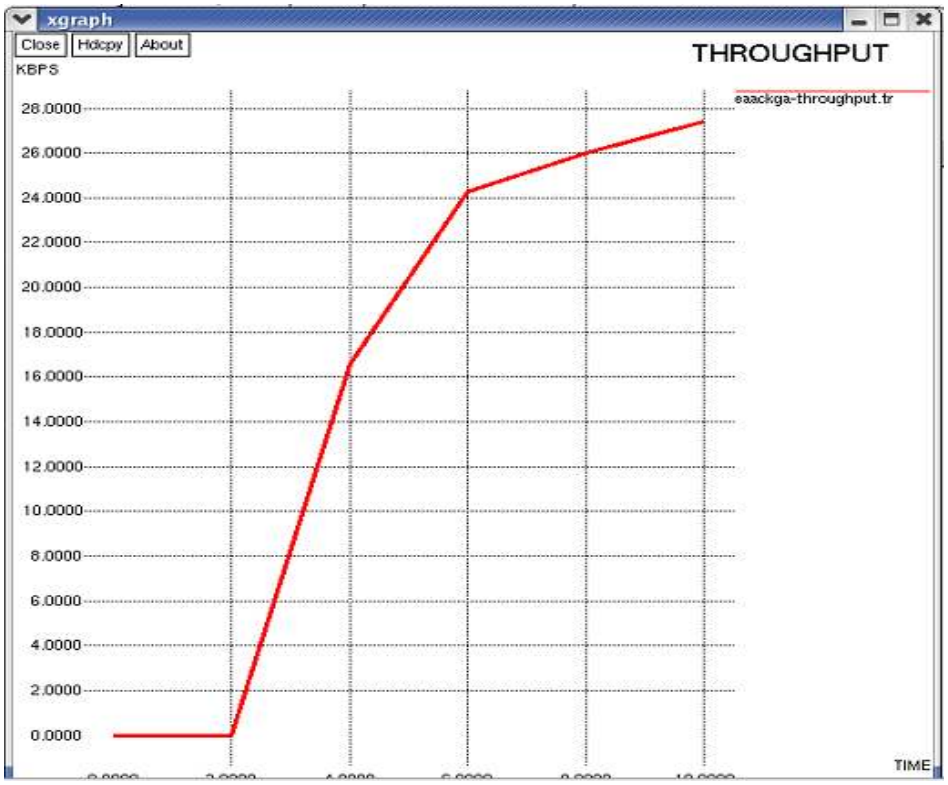

Fig. 6: Throughput graph

Throughput: In Fig. 6 Throughput is defined as the number of packet received from the source by the total number of packet sent.

Throughput: No. of packets Received/Total no. of packet sent.

CONCLUSION

In this study, we have suggested a methodology for detecting the anomalies in MANET's based on Genetic algorithm. The combination of EAACK with Genetic algorithm concept improves the QOS parameter namely delay, energy, throughput and packet delivery ratio; consequently the experimental results show reasonable performance in improvement, the malicious nodes are avoided rapidly by using the effective technique and the performance of genetic algorithm has been evaluated using NS2 simulator.

REFERENCES

Barani, F., 2014. A hybrid approach for dynamic intrusion detection in ad hoc networks using genetic algorithm and artificial immune system. Proceeding of Iranian Conference on Intelligent Systems (ICIS, 2014), pp: 1-6.

Biradar, A. and R.C. Thool, 2013. Performance of genetic algorithm based intelligent reactive protocols routing for MANET. Int. J. Adv. Res. Comput. Sci. Software Eng., 3(9).

Liu, K., J. Deng, P.K. Varshney and K. Balakrishnan, 2007. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE T. Mobile Comput., 6(5): 536-550.

Owais, S., V. Snasel, P. Kromer and A. Abraham, 2008. Survey: Using genetic algorithm approach in intrusion detection systems techniques. Proceeding of 7th Computer Information Systems and Industrial Management Applications (CISIM'08), pp: 300-307.

Shakshuki, E.M., N. Kang and T.R. Sheltami, 2013. EAACK-A secure intrusion-detection system for MANETS. IEEE T. Ind. Electron., 60(3): 1089-1098.