Volume 4, Issue 12, December 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Intrusion-Detection Based On Multiobjective Ant Colony Optimization (MACO) and Reduced Routing Overhead System for Manets

Aruna Devi. P*, D. Megala
Assistant Professor
Department of Computer Technology Department of Computer Technology
Dr.SNS Rajalakshmi College of Arts and Science

Abstract—A wireless sensor network becomes one of the frequently favored in nowadays, since of its mobility and scalable distinctiveness. From all of the WSN, one of the mainly significant networks is Mobile Ad-hoc NETworks (MANET) which is used in several numbers of the applications. One of the most important characteristic of the MANET becomes changing topology to everywhere and it should not maintain a same network infrastructure for every time. Each and every one of the nodes in the MANET is act as the transmitter and receiver, node configuration is automatically done based on the network infrastructure. Several number open issues still present in these networks among them MANET vulnerable to attacks becomes one of the most important challenging issue in nowadays. In earlier work Enhanced Adaptive Acknowledgment (EAACK) method is proposed to solve this problem in MANET ,it is easily caused by network and routing overhead problems ,still becomes less security , some of the attacks not removed in the MANET .To manage these problems in this paper presents a Ant Colony Optimization methods is proposed to perform the ACK process , proposed method the key values are generated using ant procedure during data transmission process and routing overhead problems is also solved ,thus results less attackers and less overhead results . Multiobjective Ant colony optimization (MACO) is used to solve the security problem in the MANET during data transmission that determines the attackers in the MANET and increase the security by determining the optimal key values for each user, simultaneously routing overhead also reduced in this work. Simulation results are compared to existing, EAACK, TWOACK methods it demonstrates that the proposed ACO have higher intrusion detection results and less routing overhead while does that not significantly influence the network performancesy.

Keywords—Enhanced Adaptive ACKnowledgment (AACK) (EAACK), Mobile Ad hoc NETwork (MANET), intrusion detection system, Multiobjective ant colony .

I. INTRODUCTION

Due to the characteristics of mobility and scalable, a wireless sensor network (WSN) becomes a one of the most importantly chosen network in earlier days. Because of this reduced communication cost and improved technology, WSN have increase much more attention than the wired networks during the past years. One of the most significant benefits of WSN is its capability to permit message communication among various parties and tranquil preserve their mobility. Though, this message communication is shortened to the variety of transmitters. This above mentioned problems is solved by using MANET through permit in-between party in the direction of relay message transmissions.

In converse to the conventional WSN, MANET has a decentralized network communications. MANET does not necessitate a same network infrastructure for every time; since each nodes thus, all nodes are complimentary to progress indiscriminately [1-3]. MANET is accomplished of generating a self-configuring and self-maintaining network not including the facilitate of a centralized communications, which is frequently infeasible in serious work applications similar to military disagreement or crisis improvement. Smallest design and rapid employment formulate MANET prepared toward be second-hand in emergency situation wherever a transportation is occupied or impracticable toward establish in situation approximating usual, martial conflicts, and medicinal emergency condition [4-5]. Owing to this distinctive individuality, MANET is attractive further and extra extensively implemented in the engineering [6-7].

MANET is a scheme of wireless mobile nodes with the purpose of vigorously self-organize in random and provisional system topologies [8-9]. MANET is group of WSN, which consists of huge amount of mobile nodes. As the message communication or data transmission should take place in open access medium, but it easily susceptible to safety attacks. In the presence of safety protocol influence of a variety of attacks can be concentrated. The mobile hosts vigorously create pathway in the middle of one another in arrange to converse. Consequently, the achievement of MANET data communication extremely depends on the relationship of the concerned movable nodes.

Such vitality of MANET-based architectures directs a number of intrinsic weak point and an extensive diversity of attacks intention these weak point [8]. On the other hand, in view of the fact with the intention of MANET is accepted amongst serious mission applications, network safety are of very important. But MANET easily affected by a variety of

attacks. This situation becomes fundamental to propose an intrusion-detection system (IDS) for MANETs. In this paper presents a novel swarm intelligence Multiobjective ant colony optimization (MACO) to sole the security problem in MANTEs, it becomes good for solving routing overhead problem. It is performed based on the behaviour of foraging ants thus generate a key value for each data transmission process. The communal behaviour of ants helps to discover the straight pathway starting the nest to a food source, through evidence of a substance called pheromone on the appointment nodes.

.

II. BACKGROUND KNOWLEDGE FOR BASE

Marti et al. [10] develop an intrusion detection system based on the schema called as Watchdog .The major aim of this work is to improve security result and higher throughput is achieved for MANET with higher number of malicious nodes is identified. The proposed method consists of two major parts such as Watchdog and Pathrater. Watchdog is designed as major IDS on behalf of MANETs. It is dependable used for distinguish malicious node misbehaviors in the MANET through promiscuously pay attention toward its next hop's communication.

Liu et al. [11] develops a new methods TWOACK, it becomes one of the most recently used method in earlier work for solving the IDS problem in MANET. On the opposite to a lot of other system, TWOACK is neither an improvement than Watchdog-based method. Plan to determine the recipient conflict and imperfect communication power problems of Watchdog, TWOACK distinguish disobedient associations through recognize each information transmitted in excess of each three successive nodes all along the pathway from the source to the destination.

Sheltami et al. [12] develops a new based on the TWOACK which is extension of the earlier work it is called as AACK. It is compared to existing methods and higher identification misbehavior nodes in MANET. It becomes less routing overhead and higher security results when compare to existing methods but still preserve or constant improve on the throughput for same network becomes still major issue.

Albers et al. [13] proposed a intrusion detection system for distributed environment , it is implemented in local environment so it is called as local intrusion detection System (LIDS) for every node, it should be also extended to global environment through collaborate by way of further LIDS. In order to examine the probable interruption, data should be attaining from LIDS through additional information of other nodes. Every mobile agent is able to be assigned a precise assignment which resolve in an independent and asynchronous manner with no some assist from its LIDS.

Kachirski and Guha [14] develop a multi-sensor IDS foundation on mobile agent knowledge. The scheme is able to be separated addicted to three main steps, each of which symbolize a mobile agent through positive functionality: examine, decision-making. Through unscrambling well-designed tasks addicted to group and transmission every task to a diverse agent, the workload is dispersed which is appropriately designed for the individuality of MANETs.

Buchegger and LeBoudec [15] develops a new routing protocol which is extended from DSR protocol named as Cooperation Of Nodes, Fairness In Dynamic Ad-hoc NeTworks (CONFIDANT), which is more like equal to WATCHDOG schema . Every node watches the behaviors of nearest nodes inside its radio variety and discover from them. This scheme moreover resolves the difficulty of Watchdog in routing and packet transmission. Furthermore, when nodes understanding a misbehaving node, it resolves send a notice communication to further nodes in the WSN, distinct as friends, which is relies on trusted association.

Bansal and Baker [16] also develops a new routing protocol named as DSR it is also called as Observation-based Cooperation Enforcement in Ad hoc Networks (OCEAN). It moreover makes use of a monitoring scheme and a repute scheme. Though, in distinguish to the earlier approaches on top of, OCEAN depends merely on its individual examination to pass up the innovative susceptibility of false allegation beginning used repute connections.

III. PROPOSED SECURE INTRUSION-DETECTION BASED ON MULTIOBJECTIVE ANT COLONY OPTIMIZATION (MACO) AND REDUCED ROUTING OVERHEAD METHODOLOGY

In this section, we describe our proposed MACO methods in more detail. The proposed approach extends from MACO methods to avoid the attacker beginning forging acknowledgment packets. The proposed MACO is consists of three major steps such as ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA) generation based on the MACO. In order to differentiate diverse packet category in diverse schemes, consider a 2-b packet header in MACO.

As discussed earlier, ACK is essentially an end-to-end acceptance system. It acts as a component of the hybrid system in MACO intends to decrease system overhead whilst rejection network misbehavior is identified. In Fig. 1, in ACK type, source node S initially sends a ACK to all nodes with packet data P_{ad1} to the destination node D. If each and every nodes finds a route among from source to destination nodes successfully when destination nodes receives packet data P_{ad1} from source node and if it doesn't receive then it go backs to reverse order to finds misbehavior nodes within specified time .Source node sends a packet if it is receives ack from destination node.

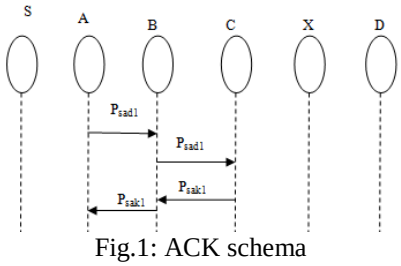

Fig.1: ACK schema

S-ACK

The S-ACK system is an enhanced description of the TWOACK system anticipated through Liu et al. [11]. The standard is to allow each three successive nodes effort in a cluster to distinguish disobedient nodes. For each one three successive nodes in the pathway, the third node is necessary to send an S-ACK response small package to the initial node. The purpose of initiate S-ACK mode is to distinguish misbehaving nodes in the existence of recipient conflict or imperfect communication power. Fig.2, S-ACK mode, the

three successive nodes (i.e., F1, F2, and F3) effort in a collection to distinguish misbehaving nodes in the system. Node F1 sends an S-ACK data packet Psad1 to node F2. Then, node F2 promotes this packet to node F3. When node F3 attains Psad1 three-node group, node F3 based on acknowledgment packet Psak1 to node F2. Node F2 forwards Psak1 back to node F1. If the corresponding node doesn't inside time period, then nodes are defined as malicious. Furthermore, a misconduct account determination created through node be F1 and send to the basis node.

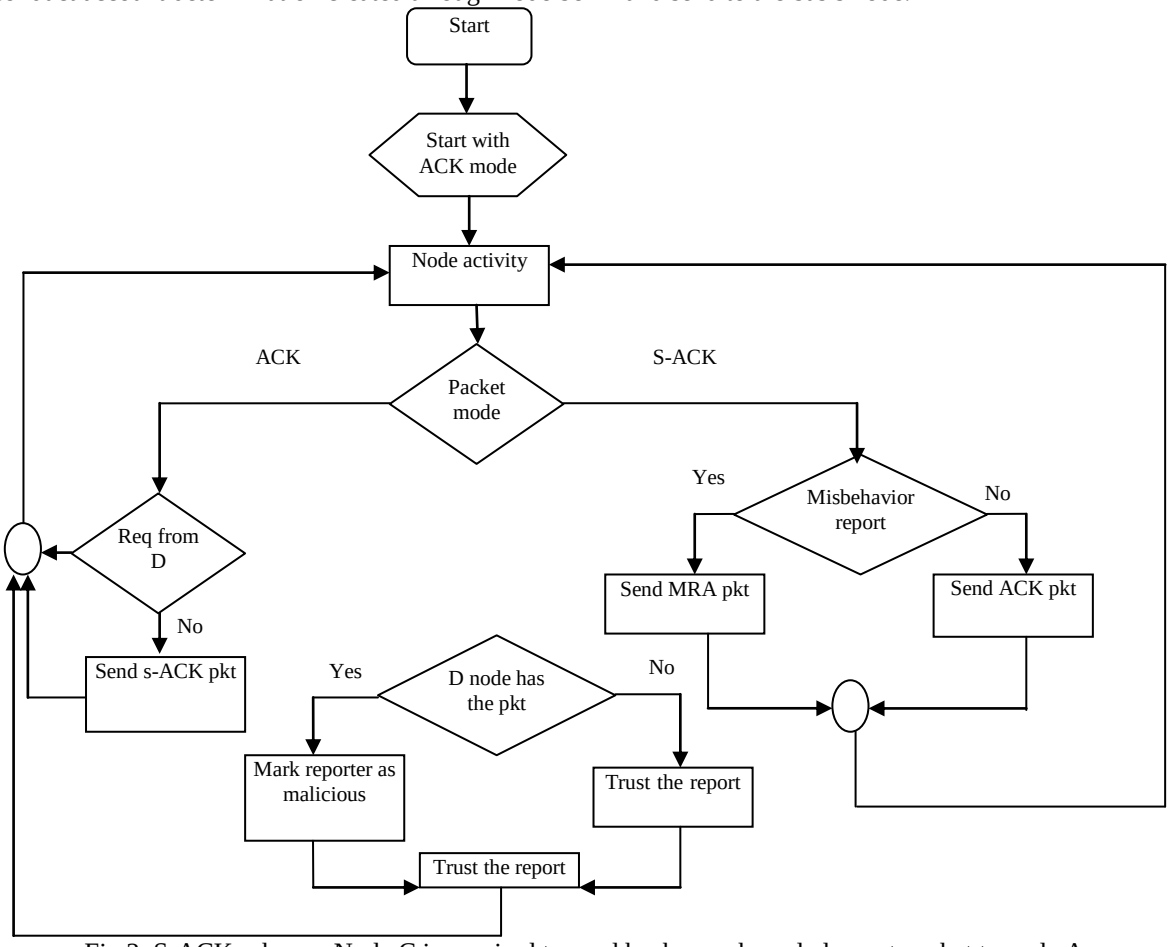

Fig.2. S-ACK scheme: Node C is required to send back an acknowledgment packet to node A

Misbehavior report authentication (MRA) generation based on the MACO

MRA based on the MACO system is planned to determination the weak point of Watchdog while it is unsuccessful to distinguish disobedient nodes through the occurrence of artificial misconduct description. The false misconduct account is able to be produce through malicious attacker to incorrectly description in the clear nodes as malicious. The central part of MRA scheme is to confirm whether the target node has received the account misplaced packet all the way through a diverse way. To begin the MRA mode, S node primary explore its neighborhood information support and look for a substitute route to the D node. If there is no route presents then starts with creation of the new ACK request and it is stored in request table. It finds numerous routes from source to destination between intermediate nodes deposit of pheromone for each one of the ant in the MANET within specified time period. $Inter_{RT}$ is an accountable routing table (RT) intended for accumulate route in the direction of a D ,if it fails then it is stored in $Intra_{RT}$ table. There are five most important fundamentals in the RT intended for an ACK pair with ACK, Pheromone, appointment times, Hops, Seq_{Num}. The pheromone ant value gets efficient through the ants as they go across the links foundation on the demand ACK. The ants transform the attention of the pheromone assessment on their crossing to the target and on their mode backside to the basis node(S). The data arrangement of the ant includes seven most important fields: Source node(S), ACK, Destination node(D), $Seq_{Num,}$ Type, Hops and Path.

Fig.3 illustrates Block diagram of multiobjective optimization for IDS in MANET. System input is number of nodes and objective measure as pheromone deposited ratio; this measure is calculated from original user requested in the ACK mode, node routing table and data structure is created under attacks.

The steps for applying MACO into scheme are Misbehavior report authentication (MRA) generation enumerated below.

(1) Define the MRA node population of ants colony size, the initial MRA node population of ants pheromone trail, the dissolving rate (σ), the objective function $\Delta\tau$, and a maximum number of iteration to stopping criterion.
(2) Using (1), create an initial MRA node population of ants in MACO , which comprise a set of probable solution. every one ant is indicate through $X = \{x_1, x_2, \ldots, x_n\}$,

$$f_{pheromone}(x_i) = e^{(x_i - x_i^*)^2/2\sigma_i^2} \quad (1)$$

σ_i^2 is the ants aggregation index for search interval.
(3) For every one ant X of the initial MRA node population, consider the following.
The ant arrangements comprise deal with fields as Source and Destination. The earlier field is dependable designed for accumulate the address of the earlier node. The H_{Info} field is accountable designed for storing the essential heuristic information to estimate the pheromone deposit ratio. The Seq_{Num} field is second-hand designed for manage. The Type field designates the ant group, and the Hops field designates the number of hops with the intention of the ant has done. While searching in favor of food, ants deposit on ground an quantity $\Delta\tau$ of individual essence called pheromone at every one visited node, anywhere,

$$\Delta\tau \propto \frac{1}{L^{\Delta}(t)} \quad (2)$$

The amount of pheromone deposited is directly measured as the worth of the route establish through the ant deposit pheromone and inversely comparative to the pathway length, $L^{\Delta}(t)$ in the route
(4) Find the best $x_{best} = (x_i^*, x_i^*, \ldots x_i^*)$ results to distinguish misbehavior and hones nodes in the MANET smallest objective value $\Delta\tau$.
(5) The pheromone values updating ,
Though the authentication of quantity of pheromone depart beginning the experimental behavior of authentic ants [17]. MANET has self-motivated topologies it is essential to extend a method designed for remove the old way. In ACO [18] this is accomplished through dissolve the pheromone exponentially at any edge (i, j) are restructured through each and every one the ants that contain finished the pathway distance end to end as follows:

$$\tau_{ij} = (1-\lambda) \times \tau_{ij} + \sum_{k=1}^{m} \tau_{ij}^{k} \quad (3)$$

where m is the total number of ants in the path or route. $\lambda \in (0,1)$ is the departure continuous that establish the departure velocity of the pheromone. τ_{ij}^{k} is the amount of pheromone placed through ant k on edge (i, j).
(6) Save the best misbehavior and honest nodes results in the generation and compare with old results .
(7) If it is reached in maximum number of iteration then the pheromone deposited ratio is checked ; else it goes to the next step.
(8) Using the uniform distribution of (1), generate a new MRA node population in MACO and then go back to 3

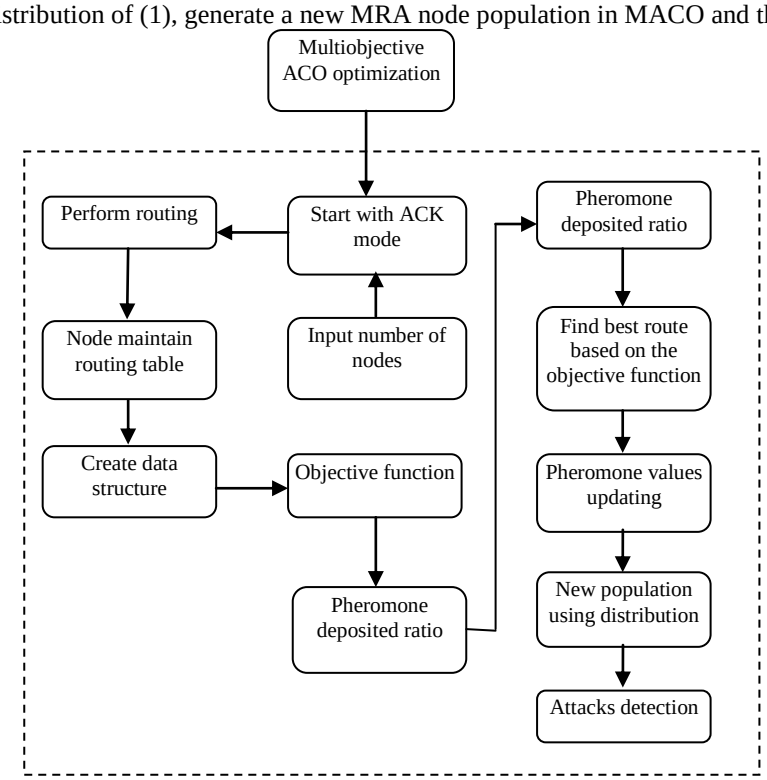

Fig. 3: Block diagram of MACO optimization for IDS in MANET

.

IV. SIMULATION RESULTS

Our simulation experimentation is carriedout based on the network simulation parameter named as Network Simulator (NS) with GCC 4.3 and Ubuntu 9.10. The proposed MACO scheme is consecutively run on various systems and on a

laptop with Intel core processor and 2-GB RAM. The purpose is to give further wide-ranging outcome and formulate it easier designed for us to evaluate the results. In network simulation parameter named as Network Simulator (NS), the default relationship indicates 50 nodes with a size of 670 × 670 m. The maximum hops permissible in this design location are four. Together the physical layer and the 802.11 MAC layer are incorporated in the WSN of NS2. The affecting rate of mobile node is restricted to 20 m/s and a suspension time of1000 s. For every one system, ran each network setting three times and designed the average performance.

In regulate to determine and evaluate the performances of our MACO proposed scheme, persist to implement the subsequent two performance metrics [13].

1) Packet delivery ratio (PDR): It is specified as the ratio of the amount of packets established through the destination node (D) to the amount of packets sent through the source node.

2) Routing overhead (RO): RO is specified as the ratio of the quantity of routing-related communication [Route REQues (RREQ), Route ERRor (RERR) ,etc].

TABLE 1: PERFORMANCE COMPARISON RESULTS

Methods	**Total number of the IP**	**Number of the spam detected**	**Confirmed**	**Missed**
SPOT	410	147	138(0.971)	9(0.29)
NMF- HC SPOT	410	157	151(0.99)	3(0.01)

TABLE I: PERFORMANCE COMPARISON FOR SIMULATION BETWEEN METHODS FOR PARAMETERS LIKE PDR,RO

METHODS	**Packet delivery ratio (PDR)**				
	Malicious nodes : 0%	**Malicious nodes : 10%**	**Malicious nodes : 20%**	**Malicious nodes : 30%**	**Malicious nodes : 40%**
TWOACK	1	0.97	0.95	0.93	0.92
AACK	1	0.97	0.96	0.93	0.92
EAACK	1	0.96	0.97	0.935	0.925
MACO	1	0.96	0.97	0.941	0.931
METHODS	**Routing overhead (RO)**				
	Malicious nodes : 0%	**Malicious nodes : 10%**	**Malicious nodes : 20%**	**Malicious nodes : 30%**	**Malicious nodes : 40%**
TWOACK	0.18	0.4	0.43	0.42	0.51
AACK	0.03	0.23	0.32	0.33	0.39
EAACK	0.15	0.28	0.35	0.44	0.58
MACO	0.1	0.15	0.23	0.25	0.45

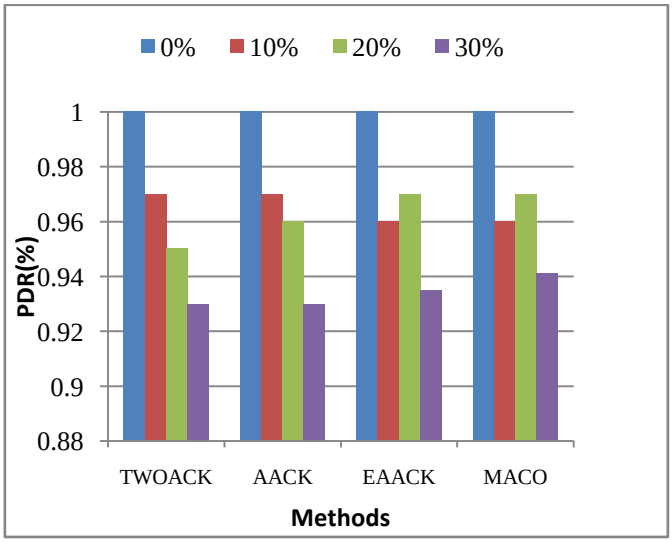

Fig.4 .Simulation results for scenario 1—PDR

Fig.4 shows the simulation results of the PDR between the methods like TWOACK,AACK,EEACK and proposed MACO methods under various percentage of the malicious nodes .if the number of the malicious node percentage increase it inversely reduces the PDR for existing methods and increase for proposed MACO method ,it shows that the

proposed work performs well than the existing methods the results are tabulated in table 1.

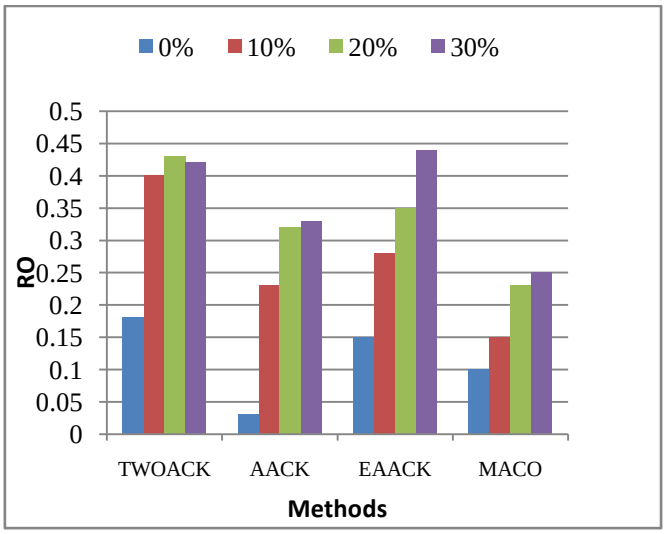

Fig.5 .Simulation results for scenario 1—RO

Fig.5 shows the simulation results of the RO between the methods like TWOACK,AACK,EEACK and proposed MACO methods under various percentage of the malicious nodes .if the number of the malicious node percentage increase the RO for existing methods also increase and decreases for proposed MACO method ,it shows that the proposed work performs well than the existing methods the results are tabulated in table 1.

V. CONCLUSION AND FUTURE WORK

Several number of attacks during data transmission from source to destination have been become a major important critical issue in MANET, to solve this problem several number of security protocols based on IDS is proposed in earlier work, among them routing overhead and security still becomes a unsolved issue .To solve these problems in this work a new swarm intelligence based Multiobjective ant colony optimization (MACO) designed to solve routing overhead and security problem in MANETs. The proposed system is named as MACO protocol particularly premeditated intended for MANETs and compared with existing EAACK, and TWOACK scenarios through simulations. Also, it must offer decentralized and adaptive routing strategies for MANET. The major aim of the proposed work is to solve security problems in the MANET and reducing routing overhead by proposing MACO based routing protocols. The results are demonstrated and compared with existing EAACK and TWOACK scenarios through simulations in the collision attack, restricted communication power, and false misconduct information.

To enhance the qualities of our investigate work; map to examine the subsequent issues in our prospect research:

1) Potential of implementing hybrid cryptography techniques to promote decrease the network overhead.
2) Observe the promise of implementing a key substitute method to remove the condition of predistributed keys;
3) Perform MACO in real time application for network environment as an alternative of software simulation.

REFERENCES

[1] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocol—A review," *J. Comput. Sci.*, vol. 3, no. 8, pp. 574–582, 2007.

[2] B. Sun, "Intrusion detection in mobile ad hoc networks," *Ph.D. dissertation*, Texas A&M Univ., College Station, TX, 2004.

[3] Tabesh and L. G. Frechette, "A low-power stand-alone adaptive circuit for harvesting energy from a piezoelectric micropower generator," *IEEE Trans. Ind. Electron.*, vol. 57, no. 3, pp. 840–849, Mar. 2010.

[4] N. Nasser and Y. Chen, "Enhanced intrusion detection systems for discovering malicious nodes in mobile ad hoc network*," in Proc. IEEE Int. Conf. Commun., Glasgow*, Scotland, pp. 1154–1159, 2007.

[5] M. Zapata and N. Asokan, "Securing ad hoc routing protocols," *in Proc. ACM Workshop Wireless Secur.*, 2002, pp. 1–10.

[6] K. Kuladinith, A. S. Timm-Giel, and C. Görg, "Mobile ad-hoc communications in AEC industry," *J. Inf. Technol. Const.*, vol. 9, pp. 313–323, 2004.

[7] K. Stanoevska-Slabeva and M. Heitmann, "Impact of mobile ad-hoc networks on the mobile value system," *in Proc. 2nd Conf. m-Bus.*, Vienna, Austria, 2003

[8] Fadlullah, Zubair Muhammad, Tarik Taleb, and Marcus Schöller. "Combating Against Security Attacks against Mobile Ad hoc Networks (MANETs)."*Security of Self-Organizing Networks: MANET, WSN, WMN, VANET* 173 (2010).

[9] Li, Wenjia, and Anupam Joshi. "Security issues in mobile ad hoc networks-a survey." *Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County* (2008): 1-23.

[10] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," *in Proc. 6th Annu. Int. Conf. Mobile Comput. Netw., Boston, MA*, 2000, pp. 255–265.

[11] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Trans. Mobile Comput.*, vol. 6, no. 5, pp. 536–550, 2007.

[12] T. Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence ofmisbehaving nodes inMANETs," *Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282, 2009.

[13] P. Albers, O. Camp, J. Percher, B. Jouga, L. M, and R. Puttini, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," *Proceedings of the 1st International Workshop on Wireless Information Systems (WIS-2002)*, pp. 1- 12, 2002.

[14] O. Kachirski and R. Guha, "Effective Intrusion Detection Using Multiple Sensors in Wireless Ad Hoc Networks," *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03),* p. 57.1, 2003.

[15] S. Buchegger and J. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks)," *Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02),* pp. 226-336, 2002.

[16] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad hoc Networks," *Research Report cs.NI/0307012*, Stanford University, 2003.

[17] K. Anuj Gupta, K. Anil. Verma, and H. Sadawarti, "Analysis of various Swarm-based and Ant-based Algorithms," in Proc. Of International Conference on Advances in Computing and Artificial Intelligence (ACAI 2011), an ACM Chapter Event, Chitkara University, Punjab, pp – 39-43.2011.

[18] M. Dorigo, M. Birattari, and T. Stutzle, "Ant colony optimization", *Computational Intelligence Magazine, IEEE,* vol. 1, no. 4, pp. 28 – 39, 2006.

[19] N. Kang, E. Shakshuki, and T. Sheltami, "Detecting forged acknowledgements in MANETs," *in Proc. IEEE 25th Int. Conf. AINA*, Biopolis, Singapore, pp. 488–494, 2011.

