A Novel Approach Against Collaborative Attacks In Manet

A.Naveena, Dr.K.Ramalinga Reddy

Assistant Professor, ETM Department, G.Narayanamma Institute of Technology and Science(for women)
Hyderabad, India

Professor and HOD, ETM Department, G.Narayanamma Institute of Technology and Science(for women)
Hyderabad, India

ambidinaveena@yahoo.com
kattareddy2000@yahoo.com

Abstract— Intrusion detection in Mobile Adhoc Network (MANET) is defined as a mechanism to detect the intruder that affects the whole network. These networks (MANET) are susceptible to many kinds of attacks because of their limited capacity such as memory, battery life, and their computational power. Anonymous communications are important for many applications of the mobile ad hoc networks (MANETs) deployed in adversary environments. A major requirement on the network is to provide unidentified and unlinkability for mobile nodes and their traffics. In this paper, a new novel approach is proposed for designing a hybrid anonymous routing protocol for organizing secure routing to minimize routing overhead and minimize energy consumption by comparing existing approach such as ALERT.

Keywords— IDS, ACO, Anonymous routing, ALERT, Authentication

I. INTRODUCTION

Mobile ad hoc networks (MANETs) are vulnerable to security threats due to the inherent characteristics of such networks, such as the open wireless medium and dynamic topology. It is difficult to provide trusted and secure communications in adversarial environments, such as battlefields. On one hand, the adversaries outside a network may infer the information about the communicating nodes or traffic flows by passive traffic observation, even if the communications are encrypted. On the other hand, the nodes inside the network cannot be always trusted, since a valid node may be captured by attackers and becomes malicious.[1]

As a result, anonymous communications are important for MANETs in adversarial environments, in which the nodes identifications and routes are replaced by random numbers or pseudonyms for protection purpose. Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers.[2] Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. For route anonymity, adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes en route.

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. ALERT is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It uses dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route.[3] But electing random relay node selection for large scale network and route selection for large scale network is not such feasible. In MANET scenario, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. To address the above-mentioned critical issues, more flexible and adaptive response should be investigated.

This paper presents novel approach to detect intruders by deploying adaptive Ant Colony Optimization technique, this technique resolve to find intruders roots, by discovering malicious routing and it provides feasible and optimal routing to IDS for identifying intruders. ACO approach organizes group nodes to detect malicious nodes by sharing its anonymity information. In order to represent anonymous communication we use hybrid authenticated anonymous securing routing protocol.[4]

In section 2 various researchers related work and the problem statements on their research are described. In section 3 the proposed model and its approach is described. In section 4
simulation and performance evaluation of proposed model is demonstrated.

II. RELATED WORK

In [5][6], data clustering methods such as fuzzy c-means and k-means have been widely used in intrusion detection system. The major drawback of this mechanism, that the clustering mechanisms are based on calculating numeric distance and the observations should be numeric. In additions its difficult to use symbolic features as a cluster and clustering mechanism consider features independently and its difficult to organize a relationship between various features in a record, in feature it degrades the attack detection rate.

In order to show an effective attack detection rate, the researchers [7], proposed layered approach using Conditional Random Fields to build an efficient IDS system which can be accomplished by implementing layered approach. The system integrates layered approach and CRFs to develop an efficient and accurate system Hop-by-hop authentication is another secure routing pattern for preventing adversaries from participating in the routing to ensure route anonymity[8][9]. MASK [10] topological routing is another authentication scheme which uses neighborhood authentication routing path discovery to anonymous secure routing and identified routes consist of valid nodes. According to Haiying and Lianyu [6], Hop-by-hop authentication and other anonymous routing protocols produces high computational cost and it failure to provide complete route anonymity protection. ALERT[11] is a new anonymous routing protocol and provide efficient anonymity protection for routes, destination and sources. ALERT uses dynamic hierarchical zone partition and randomly selects a nodes as a random relay nodes which it makes to difficult to intruders to detect end points in a route.

ANT colony Intrusion Detection System (ANTIDS) [11] is another approach to detect intruders in network. In this paper [12] SI method have been used for designing IDS, the main contribution of this research is a in depth comparison of several SI-based IDS in terms of efficiency. This presents a clear idea of which solution is more suitable for each particular case. In this paper [13] intelligent learning approach using Ant Colony Optimization (ACO) is used for identifying intrusion in the distributed network.

III. PROPOSED NOVEL AUTHENTICATION ANONYMOUS SECURED IDS BASED ON NOVEL ANT COLON OPTIMIZATION METHODOLOGY

In this proposed method of AASIDS on Novel ACO methodology to reduce routing overhead and energy consumption rate is described. This model categorize the proposed model into four major steps such as Anonymous route request, Anonymous route reply, Anonymous data transmission, and Malicious report authentication (MRA) generation based on the ACO. This model differentiate each step to illustrate secure routing and identifies misbehaved nodes. In this proposed model, the detection approach by defining anonymous routing packets is described in order to discover a route, first source sends a RREQ packet to the nodes, if the destination receives a RREQ packet then it responds to the source by sending RREP packet. To keep confidential about routing these packets are altered. The following scenarios will illustrate the proposed model approach.

3.1 Anonymous route request

This step illustrate route request packet in three different stages such as source node, intermediate node and destination node. The source node first sends its request packet by assuming destination node information, pseudonym, public key, and destination string. The destination string is represented in binary format and it consist the message about destination. The source node maintains session key, if session key expires then generates new session key, KSD to associate the source and destination. Source updates its destination information in its source destination table. Here the format of source S sending information is represented as this format

\[ S \rightarrow *: [\text{RREQ}, N_{sr}, V_{SD}, \text{Onion(S)}, G_s] \]

\[ \text{RREQ} \] is a packet type identifier; \( N_{sr} \) is a sequence number which is randomly generated by Source S for this route request; \( V_{SD} \) is an encrypted message for the request validation at the destination node; \( \text{Onion(S)} \) is a key encrypted onion created by S. The whole RREQ packet is finally signed by S with its group private key

Here \( V_{SD} \) is computed as

\[ V_{SD} = (N_v)K_v \]

\( K_v \) is represented as a symmetric key and \( N_v \) is a one time nonce for route discovery. The source use these two parameters for future route verification. The secret message is defined as

\[ V_{D} = (N_v, K_v, dest)K_{SD}(K_{SD})K_{D+} \]

Let assume D is the message receiver and It will decrypt the other part of \( V_{D} \) by its private key \( K_{D-} \). Then it obtains first part of message with \( K_{SD} \). Next the encrypted onion for source S is defined as follows
Onion(S) = OKVv(Ns)

After sending RREQ, the source updates its tables with new entry such as Nsq NSD NSD/Pending

The intermediate nodes maintain neighbor hood table with corresponding information, such as neighbor Ny and Session key. Once source node sends its RREQ to the intermediate node I, the intermediate node will verify the request packet group public key and packet signature, if the packet contains invalid information then it conclude the packet as malicious packet. The intermediate will updates its neighbor table.

Once REQ packet reaches to the destination node D, the destination validates the REQ packet similar to the intermediate node, by decrypting part of VD, it understands that it is the destination of the RREQ. D can obtain the session key KSD, the validation nonce Nv, and the validation key Kv. Then D is ready to assemble an RREP packet to reply the S’s route request.

3.2 Anonymous Route Reply

This section presents how the anonymous route replay packet organized. Once the destination node receives its packet from neighbor nodes I, then the RREP packet is defined as follows

D →*: (RREP, Nrt, (Kv, Onion(J))KSD)

Nrt is pseudonym route which is generated by Destination D. The destination D will sends its RREP to neighbor node J. The neighbor J node obtains shared keys in its neighborhood table. try to use them to decrypt (Kv, Onion(J))KSD. In case of a successful decryption, J knows the RREP is valid and from ND, and J also obtains the validation key Kv. Then J continues to decrypt the onion part. J knows the next hop for the RREP is NI. Then J will verify the linkage of the received RREP with its stored RREQ. It tries to use the obtained Kv to decrypt the verification message VSD stored in its routing table. Here we define neighbor node J’s RREP towards previous hop is as follows

J →*: (RREP, Nrt, (Kv, Onion(J))KSD)

Now source receives RREP packet from neighbor node J. The source S validates the RREP packet in similar to the intermediate node reaches S, S. If the decrypted onion core Ns equals to one of S’s issued nonce, S is the original RREQ source. S will update its routing table.

3.3 Anonymous data transmission

Once route formed across source S to destination D, now S transmit a data to the Destination D with the following data packet.

S → D: (DATA; Nrt; (Pdata)KSD)

Data is the packet type, Nrt is a pseudonym route. Pdata is data payload and it is encrypted by session key KSD. Once any node received a data, it looks into forwarding table, if Nrt matches then the data packet will be passed to the next hop. If it doesn’t matches with corresponding Nrt value then it discards the packets. Updates as a malicious data

3.4 Malicious report authentication (MRA) generation based on the ACO

Malicious report authentication (MRA) based on the ACO system is planned to determination of malicious packets. 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 explores its neighborhood information support and look for a substitute route to the D node. If there is no route present 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 routing table contains an accountable routing table (RT) intended for accumulate route in the direction of a destination D, if it fails then it is stored in IntraRT table. There are five most important fundamentals in the RT intended for an ACK pair with ACK, Pheromone, appointment times, Hops, SeqNum. 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), SeqNum, Type, Hops and Path.

(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 Δτ , and a maximum number of iteration to stopping criterion.

(2) Create an initial MRA node population of ants in ACO , which comprise a set of probable solution. every one ant is indicate through X = {x1, x2, ..., xn}.

(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 HInfo field is accountable designed for storing the essential heuristic information to estimate the pheromone deposit ratio. The SeqNum 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 a quantity $\Delta t$ of individual essence called pheromone at every one visited node, anywhere

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

(4) Find the best $X_{best} = (X_i, X_i', X_i'' ,..., X_i^n)$ results to distinguish misbehavior and honest nodes in the MANET smallest objective value $\Delta t$.

(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

(6) Save the best misbehavior and honest nodes results in the generation and compare with old results

IV. SIMULATION AND PERFORMANCE RESULTS

In this experiment, Blackhole attack is considered, this attack generally redirect the source node route and it produces malicious packets on source node packets. In this experiment we are configuring black hole attack by introducing malicious packets. The attacker interacts with source node by producing malicious packets, here secure routing management to validate nodes packets is designed. The source node verifies keys before it accepting packets, as a result the network ensures the secure routing and it defends malicious without any network interruptions. More number of malicious nodes are configured in this experiment for observing network performance. In order to evaluate the network performance key revocation process is deployed. During revocation the network successfully reduces overhead to manage key management mechanism and improves response time.

Environmental Setup Network Parameters

In this experiment 25 nodes are configured. Each node configured with defined layered network properties. AODV Routing protocol is selected and defines channels for configured network. According to the proposed method response time, energy and throughput have to improve. In order to configure secured network infrastructure, authentication process by deploying group key management scheme is defined. The performances of ALERT, and Novel AAANT approaches under different mobility scenarios is compared. Their behaviors under the packet dropping attacks with different levels is also compared.
In this paper, a novel IDS system in MANET for minimizing routing overhead and improving energy in MANET is presented. Anonymous authentication routing and ACO approach for detecting misbehaved nodes during routing process by deploying anonymous secure routing is adopted. During routing process intermediate nodes infect the routes with malicious packets, here the misbehavior nodes are detected by verifying its node anonymous information. In addition the ACO technique computes the routes inorder to
find out the misbehaved nodes by comparing its results. Ant colony optimization (ACO) is implemented to solve routing overhead and security problem in MANETs. The proposed system improved detected rate and improved the performance of routing overhead and energy with the comparison of ALERT and other ACO based IDS approaches. We extend this study for large scale networks for ensuring secured infrastructure and gain higher throughput rate for large data transmissions.

REFERENCES