Misbehaviour Detection in MANET Using H-ALARM

B Prem Kumar
M.Tech Student,
Dept. of CSSE,
Andhra University,
Visakhapatnam, AP, India.

S. Jhansi Rani
Assistant Professor,
Dept. of CSSE,
Andhra University,
Visakhapatnam, AP, India.

Abstract:

The main work of this paper is to address the security issue, because MANETs are generally more vulnerable and an extension of PRISM and ALARM protocol for MANETs, are named Heterogeneous ALARAM to Withstand DoS Attacks (H-ALARAM) based on AODV. AODV protocol is work on various modes; each mode corresponds to specific state of the node. AODV protocol is design to protect the network from malicious and selfish nodes. This project will use Extended Public key Cryptography mechanism in H-ALARAM in order to achieve security goals.

Keywords: ***Wireless Networks, AODV, MANETS, Routing misbehaviour***

1. Introduction:

Mobile Ad-hoc Network (MANET) is widely considered as one of the most important technologies for the twenty-first century. In the past decades, it has received tremendous attention from both academia and industry all over the world. A MANET typically consists of a large number of low-cost, low-power, and multifunctional wireless mobile nodes, with wireless communications and computation capabilities. These mobile nodes communicate over short distance via a wireless medium. The basic philosophy behind MANETs is that, while the capability of each individual mobile node is limited, the aggregate power of the entire network is sufficient for the required mission.

When the operating environment is hostile, as is the case in military and law enforcement settings, node identities must not be revealed. We use the term “hostile” to mean that communication is being monitored by adversarial entities that are not part of the MANET. If we further assume that genuine MANET nodes do not even trust each other (perhaps because of possible node compromise, i.e., the environment is “suspicious”), the need to hide node identities becomes more pressing. Also, in this setting, it is natural for node movements to be obscured, thus making it impossible (or, at least, very difficult) to track a node, even without knowing its identity. While such suspicious and hostile MANET environments might not be very common , they do occur in military and law enforcement domains and require high security and privacy guarantees.

In this paper, we consider what it takes to provide privacy-preserving secure communication in hostile and suspicious MANETS. We construct a protocol for Anonymous Location-Aided Routing in MANETS (ALARM) that demonstrates the feasibility of simultaneously obtaining, strong privacy, and security properties, with reasonable efficiency. Whereas, security includes node/origin authentication and location integrity. Although it might seem that our security and privacy properties contradict each other, we show that some advanced cryptographic techniques can be used to reconcile them. Based on the design of secure routing protocol SEAD on the DSDV-SQ version of the DSDV ad hoc network routing protocol. In particular, to avoid long-lived routing loops in SEAD, use destination sequence numbers, as in DSDV. This also uses these destination sequence numbers to provide replay protection of routing update messages in SEAD.

2. Related Work:

On-Demand directing conventions take a shot at the standard of making courses as and when required between a source and goal hub combine in a system topology. Our discourse is restricted to two on demand specially appointed directing conventions, AODV and AOMDV, as takes after.

2.1 Ad-hoc On-Demand Distance Vector Routing (AODV):

AODV is a responsive convention that finds courses on an as required premise utilizing a course disclosure mechanism. It utilizes customary directing tables with one section for every goal. Without utilizing source directing, AODV depends on its steering table sections to proliferate a RREP (Route Reply) back to the source furthermore to course information bundles to the goal. AODV utilizes succession numbers kept up at every goal to decide freshness of steering data and to anticipate steering circles [2]. All directing parcels convey these succession numbers.

AODV keeps up clock based states in every hub, for use of individual directing table sections, whereby more established unused passages are expelled from the table. Antecedent hub sets are kept up for each directing table section, demonstrating the neighboring hubs sets which utilize that section to course bundles. These hubs are advised with RERR (Route Error) bundles when the following bounce connects breaks. This bundle gets sent by every forerunner hub to its forerunners, adequately deleting all courses utilizing the broken connection. Course blunder spread in AODV can be pictured adroitly as a tree whose root is the hub at the purpose of disappointment and all sources utilizing the fizzled connect as the leaves [2]. The upsides of AODV are that less memory space is required as data of just dynamic courses are kept up, thusly expanding the execution, while the weakness is that this convention is not versatile and in expansive systems it does not perform well and does not support asymmetric links.

2.2 Ad-hoc On-request Multi way Distance Vector Routing (AOMDV)

Ad-hoc On-demand Multi path Distance Vector Routing (AOMDV) [9] convention is an expansion to the AODV convention for processing various circle free and connection disjoint ways [2]. The steering sections for every goal contain a rundown of the following jumps along with the relating hop counts. All the following jumps have a similar grouping number. This aides in monitoring a course. For every goal, a hub keeps up the promoted jump check, which is characterized as the most extreme jump mean all the ways, which is utilized for sending course commercials of the goal. Each copy course commercial got by a hub characterizes a substitute way to the goal. Circle flexibility is guaranteed for a hub by tolerating exchange ways to goal in the event that it has a less jump tally than the publicized jump mean that goal. Since the greatest jump number is utilized, the promoted bounce check in this way does not change for a similar succession number [2]. Whenever a course notice is gotten for a goal with a more prominent arrangement number, the following jump list what's more, the promoted jump tally are reinitialized. AOMDV can be utilized to discover hub disjoint on the other hand interface disjoint courses. To discover hub disjoint courses, every hub does not instantly dismiss copy RREQs. Each RREQs arriving by means of an alternate neighbour of the source characterizes a hub disjoint way. This is on account of hubs can't be communicate copy RREQs, so any two RREQs touching base at an middle of the road hub by means of an alternate neighbour of the source couldn't have crossed a similar hub. In an endeavour to get numerous connection disjoint courses, the goal answers to copy RREQs, the goal just answers to RREQs arriving by means of special neighbours. After the main jump, the RREPs take after the switch ways, which are node disjoint and subsequently connect disjoint. The directions of each RREP may converge at a middle of the road hub, yet each takes an alternate switch way to the source to guarantee interface disjointness [2]. The benefit of utilizing AOMDV is that it permits moderate hubs to answer to RREQs, while as yet selecting disjoint ways.

Yet, AOMDV has more message overheads amid course disclosure because of expanded flooding and since it is a multipath steering convention, the goal answers to the different RREQs those outcomes are in longer overhead.

3. ROUTING PROTOCOL:

3.1 AOMDV:

The key characteristic of an on-demand protocol is the route discovery procedure is initiated by source when needed. Whenever a traffic source needs a route, it initiates a route discovery process by sending a route request for the destination through a network-wide flood and waits for a route reply. Each route discovery flood is associated with significant latency and overhead[4]. This is particularly true for large networks. Therefore, for on demand routing to be effective, it is desirable to keep the route discovery frequency low[3]. For the proposed system AOMDV routing protocol is used. AOMDV is based on a prominent and well studied on-demand single path protocol known as ad hoc on-demand distance vector (AODV)[4].

AOMDV extends the AODV protocol to discover multiple paths between the source and the destination in every route discovery. AOMDV and AODV are having several characteristics in common. It is based on the distance vector concept and uses hop-by-hop routing approach. AOMDV also finds routes on demand using a route discovery procedure. The main difference lies in the number of routes found in each route discovery [2]. In AOMDV [7], RREQ propagation from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple RREPs traverse these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency. On demand multipath protocols discover multiple paths between the source and the destination in a single route discovery process. A new route discovery is needed only when all these paths fail. In contrast, a single path protocol has to invoke a new route discovery whenever the only path from the source to the destination fails[4]. Thus, on demand multipath protocols have fewer interruptions to the application when routes fail [4].

3.2 Performance Evaluation Metrics

We compare the performance of AODV and AOMDV according to the following performance metrics [5]:

Packet delivery ratio: the ratio of data packets delivered to the destinations to those generated by the constant bit rate.

Average End-to-End delay of data packets: this includes all possible delays caused by buffering during route discovery, queuing at the interface queue, retransmission delays at the MAC, propagation and transfer times.

Routing Overhead: the total number of routing packets transmitted during the simulation. For packets sent over multiple hops, each transmission of the packet (each hop) counts as one transmission

4. Design Goals and System Analysis

4.1 Design Goal:

I) Ensure Privacy

Identity Privacy: It consists of the following requirements:

(a) No one knows the real identities of the source and the destination, except themselves;

(b) The source and the destination have no information about the real identities of intermediate nodes en route.

Location Privacy:

(a) No one knows the exact location of the source or the destination, except themselves;
(b) Other nodes, typically intermediate nodes en route, have no information about their distance, i.e. the number of hops, from either the source or the destination. This requirement is optional, but it is desirable in keeping both identity and location anonymity of the source or the destination, especially when the distance is just one hop.

Route Anonymity:

(a) Adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination;
(b) For adversaries not in the route, they have no information on any part of the route;
(c) It is difficult for adversaries to infer the transmission pattern and motion pattern of the source or the destination;

II) Ensure Security
The protocol can protect the necessary functionalities, such as discover and maintain the route, from various types of attacks.

4.2 System Analysis:

Alarm protocol:

This section describes basic operation of ALARM and its limitations. It then outlines several extensions that mitigate such limitations. Table 2 contains the notation used to describe the ALARM protocol.

Basic Operation:

The basic steps in ALARM's operation are as follows:

1. Initialization (Offline)

a. The group manager (GM) initializes the underlying group signature scheme and enrolls all legitimate MANET nodes as group members. During this phase, each member (node) creates a unique private key (SKmember), that is not revealed to anyone. This key is needed to produce valid group signatures. It also creates a corresponding public key (PKmember), that is revealed only to the GM. In addition, each member learns the common group public key (PKGM) that is subsequently used to verify group signatures. In case of a dispute and for offline forensics, GM is responsible for opening any contested group signatures and determining actual signers.

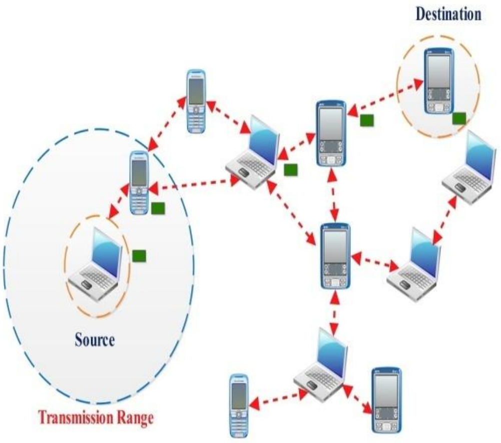


Figure 1. Mannet Topology

b. Depending on the specific group signature scheme, GM might also handle future joins for new members as well as revocation of existing members. However, in most envisaged MANET scenarios, membership is likely to be fixed, i.e., all joins can be done in bulk, before deployment. Also, revocation might not be feasible or desired, since it would require propagating—in real time— updated revocation information to all legitimate nodes. However, if dynamic membership is necessary, ALARM can support it, with minor additional assumptions

2. Operation (Online)

a. Time is divided into equal slots of duration T. At the beginning of each slot, each node s generates a temporary public-private key-pair: PK-TMPs and SK-TMPs, respectively. PK-TMPs is subsequently used by other nodes to encrypt session keys to establish secure channels with s. Note that these keys can be generated offline.

b. Each node broadcasts a Location Announcement Message (LAM), containing its location (GPScoordinates), time-stamp, temporary public key(PK-TMPs), and a group signature computed over these fields. Each LAM is flooded throughout the MANET. LAM format used to construct the network topology snapshot in Fig. 1. The sequence of steps required for sending a LAM.

c. Upon receipt of a new LAM, a node first checks that it has not received the same LAM before; it then verifies the time-stamp and group signature. If both are valid, the node rebroadcasts the LAM to its neighbors. Having collected all current LAMs, each node constructs a geographical map of the MANET and a corresponding node connectivity graph. A flowchart describing this sequence of steps. Between successive LAMs, a node can be reached (addressed) using a temporary pseudonym formed as current location concatenated with the group signature in the last LAM (TmpID ¼ fLocationkGSigg). Note that the pseudonym represents a valid address even if the actual node moves in the interim. The location is included in the pseudonym in order to minimize required state and assist in the forwarding process.3 If the location is not part of the pseudonym, a node forwarding a message to a pseudonym would have to look up the associated location and decide how to forward to that location. (See below for more details on the forwarding process). Including location in the pseudonym speeds up the forwarding process and requires fewer look-ups.

d. Whenever a node desires to communicate with a certain location, it checks to see if any node currently exists at (or near) that location. If so, it sends a message to the destination's current pseudonym (TmpID). This message is encrypted with a session key using a symmetric cipher. The session key is, in turn, encrypted under the current public key (PK-TMP) included in the destination's latest LAM. When the destination receives the message, it first recovers the session key and uses it to decrypt the rest. ALARM is not restricted to any specific public key technique. One obvious choice is Diffie-Hellman (DH), whereby each LAM includes an ephemeral (period-specific) DH half-key. The sender then simply generates its own DH half-key, computes a shared key and encrypts the session key with it. Clearly, the sender's half-key must be included in the clear-text part of the message. Other key agreement schemes can also be used. The sequence of steps involved in determining a destination node.

e. Forwarding: As described above, nodes disseminate current topology by periodically flooding LAMs. Once each node has the entire topology view, it decides whether to communicate with a certain location (node). Message forwarding is independent of topology dissemination. One option is for a node to create a source route, explicitly encoding locations of nodes on the path to the destination. The actual path can be computed using the shortest path algorithm or any other location-aided routing algorithm For example, consider the simple topology of Fig. 1. Assume that the node at location1 (TmpID1 ¼ fLocation1kGSig1g) requires sending a message to another node at location4 (TmpID4 ¼ fLocation4kGSig4g). The sender calculates the route to location4 and determines that it has to pass through location2 and location3. It then generates a session key (Ks) and encrypts data with that key using a symmetric cipher (e.g., AES). It then uses the public key in the last LAM of location4 to encrypt Ks and assembles a data message with the destination set to (TmpID4) and source—to (TmpID1). It finally composes a source route: < TMPID2; TMPID3 >.

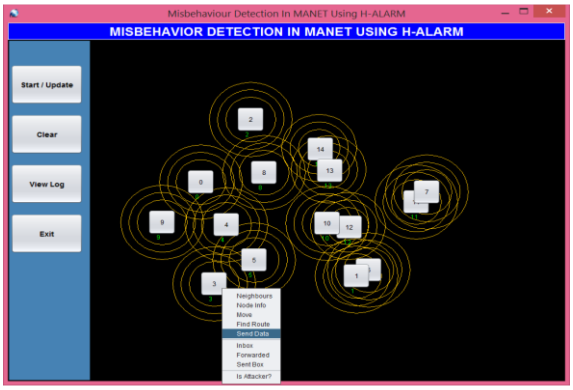
3. Forensics (Optional, offline). Each node logs all sent and received LAMs (except duplicates). Collectively, this information constitutes an operational log that is, after each field deployment, transferred to an offline server, e.g., GM. All LAMs collected by all nodes are then reconciled and, in the process, all group signatures are verified and opened by GM. Each group signature's originator is thus identified. This process allows most insider misbehavior, such as Sybil attacks, to be detected post factum. The only insider attacks that might not be identifiable using logs is location fraud. In general, operational logs are used for accountability purposes by allowing GM to reconstruct the exact sequence of node movements and topology

snapshots. We stress that this is an optional procedure that does not incur any additional overhead (beyond storage) during online operation of ALARM. Assuming LAM size of 350 bytes (8 for location, 4 for time-stamp, 128 for temporary key, and 200 for short group signature a network of 100 nodes deployed for a week and topology update frequency of 10 LAMs per minute, combined storage for all operational logs would amount to around 3.5 GB.

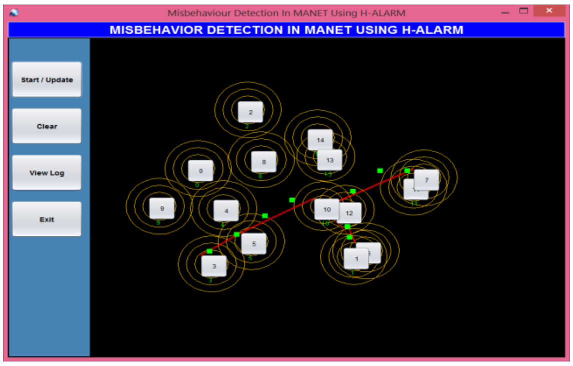
4. ALARM Limitations. The main advantage of the basic ALARM protocol is its simplicity and effectiveness.

5. Results:

The below figures shows the number of nodes used to process the project. We calculate the neighbours for each node and the range between one node to the other.



The below figure shows sending of message from one node to the other node


Misbehaviour Detection In MANET Using H-ALARM
MISBEHAVIOR DETECTION IN MANET USING H-ALARM
Start / Update
Clear
View Log
Exit
2
14
13
0
8
7
9
4
10
12
5
3
1

6. Conclusion:

This paper presents the H-ALARM protocol which supports anonymous reactive routing in suspicious location-based MANETs. It relies on group signatures to authenticate nodes, ensure integrity of routing messages while preventing node tracking. It works with any group signature scheme and any location-based forwarding mechanism. We evaluate its routing overhead and show that it can outperform anonymous link state based approaches under certain traffic patterns. We also evaluate H-ALARM's tracking-resistance by comparing its degree of topology exposure to link-state based approaches. H-ALARM reveals less of the topology and is thus more privacy-friendly. In the future, plan to study the impact of our "test suite" on the performance of other ad hoc network protocols like multicast ad hoc, geographic routing protocols. This study would help to understand the impact of mobility more deeply and clearly. Several parameters such as traffic patterns, node density and initial placement pattern of nodes may affect the routing performance and need to investigate them further. It will aim at improving the efficiency of ASR in the terms of route changes. One possible extension is to provide the functionality of repairing broken routes locally without compromising anonymity and security. In future work, consider mechanisms to detect and expose nodes that advertise routes but do not forward packets, and to merge this work with other working securing on-demand routing protocols to create a secure protocol based on ZRP.

References:

[1]. S.N.Chobe, Deepali Gothawal, " An Acknowledgement Based Approach For Routing Misbehavior Detection In Manet With Aomdv", International Journal of Advanced Computational Engineering and Networking, Volume- 1, Issue- 5, July-2013.

[2]. H.D.Trung, W.Benjapolakul, P.M.Duc, "Performance evaluation and comparison of different ad hoc routing protocols", Department of Electrical Engineering, Chulalongkorn University, Bangkok, Thailand, May 2007

[3]. Jakobsson, M. and Hubaux, J.P. and Butty, "A micro-payment scheme encouraging collaboration in multi-hop cellular networks", Computer Aided Verification, pages=15–33, year=2003, organization= Springer

[4]. Liu, K. and Deng, J. and Varshney, P.K. and Balakrishnan, K.,"An acknowledgment-based approach for the detection of routing misbehavior in MANETs", Mobile Computing, IEEE Transactions volume=6, number=5, pages=536–550, year=2007, publisher=IEEE.

[5]. H.D.Trung, W.Benjapolakul, P.M.Duc, "Performance evaluation and comparison of different ad hoc routing protocols", Department of Electrical Engineering, Chulalongkorn University, Bangkok, Thailand, May 2007

[6] L.B.Oliveira, I.G.Siqueira, A.A.F.Loureuro,"On the performance of ad hoc routing protocols under a peer-to-peer application", Computer Science Department, Federal University of Minas Gerais, Brazil, July 2005

[7] T.Fujiwara, T.Watanbe, "An ad hoc networking scheme in hybrid networks for emergency communication", Information Technology Lab, Eugene Co. Ltd, Hamamatsu, Shizuoka, Japan

[8] P.P.Pham, S.Perreau, "Increasing the network performance using multi-path routing mechanism with load balance", Institute of Telecommunications Research, University of South Australia, Australia, September 2003

[9] M.K.Marina and S.R.Das, "On-Demand multipath distance vector routing in ad hoc networks" in: Proceedings of the 9th IEEE

[10] C.S.R.Murthy, B.S.Manoj, Ad hoc Wireless Networks, Architecture and Protocols, 6th Edition.

[11]. R.Balakrishna, M.Murali Mohan Reddy Dr.U.RajeswarRao,Dr.G.A.Ramachandra, "Routing Misbehavior Detection in MANET Using 2ACK", in IEEE Advanced Computing Conference, Thapur University, Patala,2008.

[12] R.Balakrishna, M.Murali Mohan Reddy, Dr.U.Rajeswar Rao, Dr.G.A.Ramachandra," detection of routing misbehavior in mobile ad hoc networks using enhanced 2ack (e-2ack)",in IEEE Advanced Computing Conference in at , Thapur University, Patal,2008.

[13].R.Balakrishna, Dr.U.Rajeswara Rao, Dr.N.Geethanjali, "Secure Key Exchage protocol for Credential Services", Published in Defence science Jounal in May 2009.

[14].R.Balakrishna, Dr.U.Rajeswara Rao, Dr.N.Geethanjali "A secured authenticated key exchange protocol for credential services", in 3rd International conference ICACCT-2008, Page 120-129,www.apiitindia.org/icacct2008.

[15] R.Balakrishna , Dr.U. Rajeswara Rao, Dr.N.Geethanjali,"Video Conferencing on Mobile Ad-hoc Network", in 2nd International Conference CCR2008,Page298-305.

Author Details

B. Prem Kumar pursuing his M.Tech in the department of Computer Science and system Engineering, Andhra University, Visakhapatnam, A.P., India.. He obtained his B.Tech(CSE) from Narsaraopet Engineering College, Narsaraopet, Guntur.

S Jhansi Rani, M.Tech, working as Assistant Professor in the department of Computer Science and Technology, Andhra University, Visakhapatnam, A.P., India .Her area of interest computer networks and image processing.