



SECURE ROUTE DISCOVERY FOR DYNAMIC SOURCE ROUTING IN MANETs

¹ M.Anto Bennet, ¹ G.Vijayalakshmi, ² P.Shenbagavalli, ² M.Vijayalakshmi, ² S.Saranya

¹ Faculty of Electronics and Communication Department, vel tech, Chennai, India.

² UG Students of Electronics and Communication Department, vel tech, Chennai, India.

* Email: bennetmab@gmail.com

Submitted: May 27, 2017

Accepted: June 15, 2017

Published: Sep 1, 2017

Abstract- Mobile ad hoc networks (MANETs) are collections of wireless mobile devices with restricted broadcast range and resources and no fixed infrastructure. Communication is achieved by communicating data along suitable routes that are dynamically discovered and maintained through association between the nodes. Discovery of such routes is a major task both from good organization and security points of view. Recently a security model tailored to the specific requirements of MANETs. A novel route discovery algorithm called endairA is also proposed together with a claimed security proof within the same model. In this paper we show the security proof for the route discovery algorithm endairA is malfunctioning and moreover this algorithm is vulnerable to a hidden channel attack. We also analyze the security framework that is used for route discovery and argue the compos ability is an essential feature for ubiquitous applications. We conclude by discussing some of the major security challenges for route discovery in MANETs.

Index terms: Fast Mobile ad hoc networks (MANETs), Message Authentication Codes(MACs),Source Routing Protocol(SRP)

I. INTRODUCTION

Our main involvement in this work is to show the security proof for endairA given in blemished and that this routing algorithm is similarly subject to a hidden channel attack. Revisiting the ABV model we present several reasons we think the concurrent security for MANET route discovery i.e. the ABV model's security standardize insouciant in practice because it requires the absence of channels that are always present in any real-world MANET application. We can argue the higher security standard namely compos ability is a fundamental requirement for omnipresent applications. We make some observations about issues that have to be addressed by any routing protocol achieves security in a compos able model. We review route discovery and the Ariadne protocol we show the security authentication for endairA is terrified[1]. This algorithm is subject to a concealed channel attack. We discuss the significance of concurrency-based attacks and the requirements for a formal security framework for MANETs. We discuss challenges for secure route discovery and we summarize our arguments for provable security in MANETs. Mobile ad hoc networks are collection of wireless mobile devices with restricted broadcast range and resources, no fixed infrastructure .Interrelated collection of wireless nodes enter and leave over time. In also act as routers and forward packets which has no pre-established network infrastructure and there is no centralized management and no preexisting infrastructure. In MANETs all hosts are mobile and Lack well pre-defined relationship. In this the Power constraint and limited computational capability are used in the ad hoc networks. Where the Hosts communicate through the wireless links which means the radio channels and the Hosts oblige to route packets within the network itself. Routing is important that the route discovery can be changed in any order which is no fixed infra structures [7, 8, and 9].

Several attempts have been made to address the security of MANET route discovery more robustly, the most recent one being introduced in a series of papers by [2], and [3, 4,].In these works, the authors develop a formal idealization and simulation framework that adapts ideas from the secure reactive systems approach and the universally composable security approach to the realm of MANET applications[5,6].

II. PERSONALITY OF MANETS

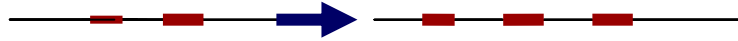


Fig:1 Personality of MANETs

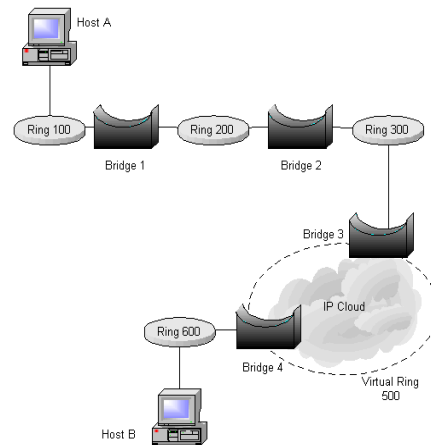
In personality of manets the dynamic Topologies and node memberships plays vita role. Where the Bandwidth is limitations and there will be Many broadcast Errors due to there no fixed infra structure .The Energy-constrained function is more shown in fig 1.

III. MANETS AND THE INTERNET

In both the mobile ad hoc networks and in internet the Future goal is faultless net connectivity because due to the infra structure. Where the mobile IP requests to be modified according to the users and the common interfacing between Bluetooth, WAP and IP are connected to the user applications need for handheld and moveable computing devices. where ad hoc networks and internet both provides security to their users during the connection. The nodes of a MANETs routers that build up routes dynamically and insert into the wireless topologies.

IV. PROPOSED WORK

Bridges operate in both the physical and the data link layer of the OSI model .Bridges can divide a large network into smaller segments. Bridges can also provide through this partitioning of traffic. A bridge operates at the data link layer, giving it access to the physical addresses of all stations connected to it. When a frame enters a bridge, the bridge not only regenerates the signal but checks the address of the destination and forwards the new copy only to the segment to which the address belongs.(Fig:2)

**Fig.2 Architecture Diagram**

As a bridge encounters a packet, it reads the address contained in the frame and compares that address with a table of all the stations on both segments. When it finds a match, it discovers to which segment the station belongs and relays the packet only to that segment. In a ring topology, each device has a dedicated point to point line configuration only with the two devices on either side of it. A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates the bits and passes them along. A packet from host A addressed to host B arrives at the bridge. host A is one of the same segment as host B, therefore the packet is blocked from crossing into the lower segment instead the packet is relayed to the entire upper segment and received by the host B.

V. ROUTING ALGORITHMS

Route discovery is initiated by a source node S that requests from its neighbors information can be used to find a route that links it to a target node T. The neighbors of S forward the request to their neighbors who in turn forward it to their neighbors and so on until eventually a route that links S to T is discovered. All nodes on a route other than S; T are called intermediate nodes. There are two general types of route discovery: proactive and reactive or on-demand. Proactive routing is usually table driven: nodes maintain routing tables with routing information to potential target nodes. The tables are updated at regular intervals, and are used by intermediate nodes for route discovery. With reactive algorithms, routes are discovered only when needed. Proactive routing is network-centric, and is appropriate for networks with heavy communication

trace for which security is not critical. Reactive routing is source-centric: intermediate nodes are restricted to forwarding and possibly verifying route requests or route responses. From a security point of view, reactive (on-demand) routing is preferable because the security is to a large extent centralized (managed by the source). Proactive routing is network-centric and appropriate for networks with heavy communication traffic for which security is not critical. Indeed, such routing strategies tend to rely on link-to-link security which implies trust in intermediate nodes. Reactive routing is source-centric: intermediate nodes are restricted to forwarding and possibly verifying route requests or route responses. From a security point of view, reactive (on-demand) routing is easier to analyze for its security properties because the security is end-to-end (managed by the source and target).

VI. SOURCE ROUTING PROTOCOL (SRP)

SRP is an on-demand source routing protocol that captures the basic features of reactive routing. In SRP route requests generated by a source S is protected by MACs (Message Authentication Codes) computed using a key shared with the target T . Requests are broadcast to all the neighbors of S . Each neighbor that receives a request for the first time appends its identifier to the request and re-broadcasts it.

Intermediate nodes do the same. The MAC in the request is not checked because only S and T know the key used to compute it. When this request reaches the target T , its MAC is checked by T . If it is valid then it is assumed by the target that all adjacent pairs of nodes on the path of the route request are neighbors. Such paths are called valid or plausible routes. The target T replaces the MAC of a valid route request, by a MAC computed with the same key that authenticates the route. This is then sending back (upstream) to S using the reverse route.

A route request that reaches an intermediate node X_j is of the form:

$$\text{VII. } \text{Msgs, } T, \text{ rreq} = (\text{rreq, } S, T, \text{id, } S_n, X_1 \dots X_j; \text{macs});$$

With id a randomly generated route identifier, s_n a session number and mac_S a MAC on $(\text{rreq}; S; T; \text{id}; s_n)$ computed by S using a key shared with T . If S, X_1, \dots, X_p, T is a discovered route, then the route reply of the target T has the following fixed form for all intermediate nodes $X_j, 1 \leq j \leq p$. fixed form for all intermediate nodes $X_j, 1 \leq j \leq p$.

VIII. $\text{MsgS, T, rrep} = (\text{rrep, s, t, id, sn, } x_1 \dots x_p, \text{macT});$

Where macT is a MAC computed by T with the key shared with S on the message field preceding it. Intermediate nodes should check the route reply header (including its id and sn) and those they are adjacent with two of their neighbors on the route before sending the route reply upstream.

Observe that even though the upstream route from T to S is authenticated by the target, the downstream route (S to T) is not. Consequently faulty node pairs (X_j, X_{j+1}) that are adjacent on the route may not be neighbors, but may divert extra c via other routes. The faulty nodes need not include the details of these routes in the route request. It is similarly possible for a malicious node to pad route requests with the identities of other nodes that are not its neighbors and impersonate these nodes in the reply phase. The resulting route therefore may not be valid in the sense that some of its adjacent nodes may not be neighbors.

IX. ARIADNE

ARIADNE is an on-demand routing algorithm based on the Dynamic Source Routing (DSR) protocol. There are several variants of Adriane depending on which mode of authentication is used to protect route requests: one uses digital signatures and one uses MACs. The MAC versions have an optimized variant uses iterated MAC computations instead of several independent MACs.

X. Basic Ariadne Route Discovery

We present the design of the Ariadne protocol in three stages: we first present a mechanism that enables the target to verify the authenticity of the route request; we then present three alternative mechanisms for authenticating data in route requests and route replies; and finally, we present an efficient per-hop hashing Technique to verify that no node is missing from the node list in the request. In the following discussion we assume that the initiator] performs S.A Route Discovery for target D, and that they share the secret keys K_{SD} and K_{DS} respectively, for message authentication in each direction. A typical route request that reaches an intermediate node A_x , $1 \leq j \leq p$, on the route $S = X_0, X_1, \dots, X_p, X_{p+1} = T$ is Of the form

$$\text{msg}_{S,T, \text{freq.}} = (\text{freq.}, S, T, \text{id}, X_1, \dots, A_x, \text{mac}_{SX_1 \dots A_x}),$$

Where $\text{macS}_{x1} \dots A_x$ is the MAC computed by A_x with a key it shares with T on the route request received from A_x .

XI. Target authenticates route requests

To convince the target of the legitimacy of each field in a route request the initiator simply includes a MAC computed with key K_D over unique data for example a timestamp. The target can easily verify the authenticity and freshness of the route request using the shared key K_S .

XII. Three techniques for data authentication

In a route discovery, the initiator wants to authenticate each individual node in the node list of the route reply. A secondary requirement is that the target can authenticate each node in the node list of the route request so that it will return a route reply only along paths that contain only legitimate nodes. We present three alternative techniques to achieve node list authentication: the TESLA protocol digital signatures and standard MACs. In our design, we assume that a sender trusts the destination with which it communicates, for authenticating nodes on the path between them. This assumption is straightforward, as the destination node can control all communication with the sender anyway. The destination node can potentially blackmail nodes on the path to the sender. The sender thus needs to keep a separate blacklist for each destination.

XIII. ANALYSIS OF ARIADNE

This framework is used to analyze SRP and Ariadne finding them insecure against hidden-channel attacks, and led to the design of endairA an on-demand route discovery protocol that the authors claim to be provably secure. The security framework which we refer as the ABV model. A proof of the security claim for endairA is also given in the analysis.

XIV. THE ABV MODEL

In the generic secure reactive system approach but there are some crucial differences. In the ABV framework: The adversary does not have full control of message delivery schedule, in the sense that the broadcast channel enforces the concept of communication rounds in particular, the ABV framework does not capture rushing attacks (synchrony) The adversary may prompt honest

Secure route discovery for dynamic source routing in manets

parties to initiate new route discoveries but not dishonest ones in other words the ABV security framework does not capture concurrent security in the presence of route discovery sessions that are initiated by adversarial nodes. The adversary is non-adaptive, i.e., cannot initiate new route discoveries as a function of previously observed messages or for these restrictions. The link configuration G_V , EP , V , L_P of an MANET is enforced in the security framework by the communication medium functionality (Machine C in the real-world model of ABV). These approaches compare executions of a protocol in a real-world model to its executions in an ideal-world model that is controlled by the functionality F , which captures formally the goals that is supposed to achieve. In the real world, the adversary is modeled as a traditional Byzantine adversary of the Dolev-Yao model, i.e., it is able to Schedule and tamper with all communication channels to provide inputs to honest parties and observe their outputs, 1 and coordinate the actions of all corrupted parties. Additionally, the adversary is capable of interacting with other sessions of the protocol that may be executing concurrently.2 the ideal-world adversary mimics the behavior of the real-world one to allow for simulations of real-world protocol executions in the ideal world. In order that be secure in this framework, the effects on the execution of in the real-world model by any real-world adversary A should be indistinguishable from those of an appropriately chosen ideal-world adversary A_0 in the ideal world model.

XV. Ariadne: Prevent Route Request Flood

DoS Attack: Impersonate other nodes and issue Route Requests Solution: Use one-way hash chain and disclose new element in each Route Request, similar to S/Key Attacker can at worst produce as many Route Requests as sender.

XVI. Ariadne: Prevent Hop Drop

Source and destination share KSD. Source adds $h_0 = \text{MAC}(KSD, \text{request})$. Every hop computes $h_i = H(\text{Node id} \parallel h_{i-1})$ (H is one-way cryptographic hash function) Destination computes h_0 reconstructs each h_i Attacker cannot drop nodes from address list in Route Request.

XVII. Ariadne: Route Authentication

Use TESLA to authenticate each hop. Every hop adds a MAC to Route Request. Destination verifies security condition. Every hop discloses key in Route Reply. Source can authenticate all hops.

XVIII. EndairA – a secure source routing protocol

Target verifies:

There's no repeating ID in the node list last node in the node list is a neighbor each intermediate node verifies its own ID is in the node list and there's no repeating ID in the node list. Then the next and previous nodes in the node list are neighbors each other .Where all signatures are valid and correspond to the nodes in the node list itself.

Source verifies:

There's no repeating ID in the node list first node in the node list is a neighbor each node verifies its own node list all signatures are valid and correspond to the nodes in the node list shown in fig 3.

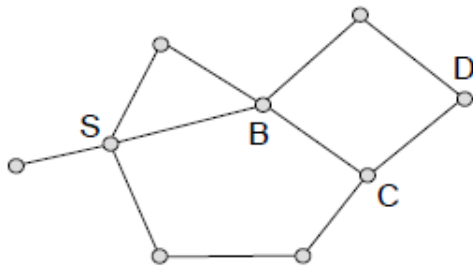


Fig.3 Node list

$S \rightarrow * : [\text{rreq}, S, D, \text{id}, ()]$

$B \rightarrow * : [\text{rreq}, S, D, \text{id}, (B)]$

$C \rightarrow * : [\text{rreq}, S, D, \text{id}, (B, C)]$

$D \rightarrow C : [\text{rrep}, S, D, (B, C), (\text{sigD})]$

$C \rightarrow B : [\text{rrep}, S, D, (B, C), (\text{sigD}, \text{sigC})]$

$B \rightarrow S : [\text{rrep}, S, D, (B, C), (\text{sigD}, \text{sigC}, \text{sigB})]$

XIX. PROVABLE SECURITY FOR AD HOC NETWORK ROUTING PROTOCOLS

Several “secure” routing protocols have been proposed for wireless ad hoc networks .SRP, Ariadne, S-AODV, ARAN, SEAD.Their security have been analyzed mainly by informal means. Informal reasoning about security protocols is prone to errors and lessons learnt in the field of key exchange protocols. Where some attacks have been found against SRP, Ariadne, and S-

AODV. Then we need more assurances about mathematical models, precise definitions and sound proof techniques shown in fig 4.

XX. AN ATTACK ON ARIADNE

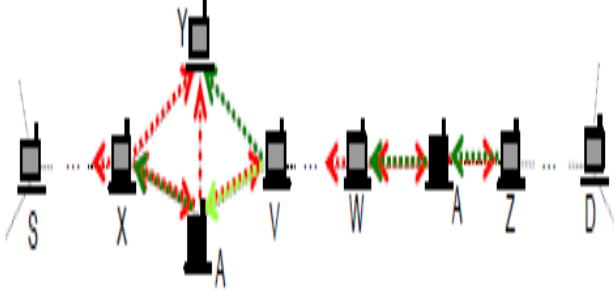


Fig.4 ATTACK ON ARIADNE

$X \rightarrow * : [\text{RREQ}, S, D, \text{id}, hX, (\dots, X), (\dots, \text{macXD})]$

$A \rightarrow * : [\text{RREQ}, S, D, \text{id}, *, (\dots, X, A), (\dots, \text{macXD}, hX)]$

$W \rightarrow * : [\text{RREQ}, S, D, \text{id}, *, (\dots, X, A, V, \dots, W), (\dots, \text{macXD}, hX, \dots, \text{macWD})]$

$A : hA = H(A \mid hX)$

$A \rightarrow * : [\text{RREQ}, S, D, \text{id}, hA, (\dots, X, A), (\dots, \text{macXD}, \text{macAD})] \dots \dots$

$Z \rightarrow A : [\text{RREP}, D, S, (\dots, X, A, Z, \dots), \text{macDS}]$

$A \rightarrow W : [\text{RREP}, D, S, (\dots, X, Y, V, \dots, W, A, \dots), \text{macDS}] \dots \dots$

$V \rightarrow Y : [\text{RREP}, D, S, (\dots, X, Y, V, \dots, W, A, \dots), \text{macDS}]$

$A \rightarrow X : [\text{RREP}, D, S, (\dots, X, A, Z, \dots), \text{macDS}] \dots \dots$

$? \rightarrow S : [\text{RREP}, D, S, (\dots, X, A, Z, \dots), \text{macDS}]$ (a non-existent route!)

XXI. CONFIGURATION

An ad hoc network is represented by a graph $G(V, E)$, where the V : vertices are network nodes (honest and adversarial) E : edges represent communication links (radio or wormhole) $V^* \subset V$ is a set of distinguished nodes (under the adversary's control). L is a labeling function (assigns IDs to nodes) with the following restrictions: Each honest node has a unique, uncompromised ID. Each adversarial node is labeled with all the compromised IDs shown in fig 5. They assume that

ID's are authenticated during neighbor discovery (Sybil attack is excluded) a configuration is a triplet: (G, V^*, L) .

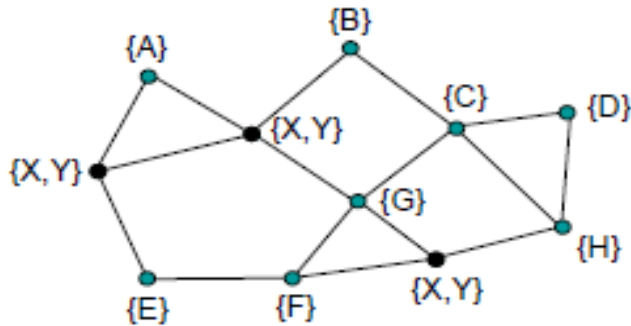


Fig.5 Configuration triplet

XXII. Hidden Channel and Concurrency Attacks

There are other channels that in many respects are much more natural. Indeed, the main objective of a route discovery algorithm is to find a route that is a suitable communication channel. Route discovery per se makes little sense. It would, therefore, be natural for nodes to use for their communication a route that was discovered earlier, whatever their intention. Therefore, it is unreasonable to restrict nodes from using hidden channels. Note that privacy is a legitimate goal for secure communication, so intermediate nodes should expect to retransmit the encrypted data. Let us now pursue our earlier discussion on interleaving protocol instances. In a networking environment, one should expect that several instantiations of a routing protocol are executed. Some may involve route discovery, while others route maintenance, data communication, or general network applications. It makes no sense to require that route communication can only start when all the other route discovery instantiations (and network applications) have been completed. Indeed, this argument should be carried to its logical extension: the security of any protocol should not be considered in isolation, but in the presence of Concurrent executions, i.e., whether these involve the same protocol or other protocols. Consequently, in our adversarial model, we should allow the adversary to interleave instantiations of several protocols, all running concurrently. This is a natural requirement for security.

XXIII. The Adversary

Secure route discovery for dynamic source routing in manets

It is sometimes suggested that adversarial nodes should be bound by the same constraints as non adversarial nodes, for example, have similar communication capabilities . This may be the case for some applications, but it is not realistic. Although, it may seem reasonable to assume that the resources of adversarial nodes are (polynomials) bounded, allowing for the constraints on ubiquitous applications, it is unreasonable to assume that adversarial nodes cannot use more powerful transmitters than non adversarial nodes. say transmitters that are 50 percent more powerful than the norm 5 if with such means they can compromise the system.

XXIV. Compensability Issues:

We argue that compos ability is an essential requirement for secure routing in MANETs. Indeed, MANETs can distinctly be characterized from fixed-infrastructure networks by the fact that both the control plane (routing messages) and the data plane (proper communication messages) are highly subject to a variety of attacks. It becomes essential to understand how the security requirements of each layer interfere with each other. The packet is therefore discarded at the SSL layer. However, since it was already accepted at the TCP layer, and moreover, has arrived earlier than the legitimate packet from the original sender, it will prevent TCP from accepting the latter (legitimate) packet. This is because the TCP daemon has recorded that packet's sequence number as already received. The SSL session layer fails to recover the missing data, and therefore, SSL+TCP do not provide availability guarantees. In this scheme, TCP provides availability but not integrity. SSL provides integrity but relies on the availability properties of TCP. This reliance proves unfounded, as the availability guarantees of TCP are only provided under the weaker integrity notion corresponding to verifiability of the TCP checksums. Composability fails accordingly. MANET routing security presents very similar problems. Indeed, as has been demonstrated by the designers of the endairA protocol, even the provision of a single property (safety of routing discovery) requires at least a concurrent approach, as illustrated by the attacks on Ariadne . We extend this observation by remarking that special care needs to be taken when assuming properties of lower network layers, especially when such properties are achieved under restrictions.

XXV. SECURE ROUTE DISCOVERY CHALLENGES

Our argument about the impossibility of secure discovery of routes is simple and has been articulated throughout the project. We base it on the fact that every route discovery algorithm is,

in practice, vulnerable to attacks that exploit alternative communication channels to articulate distributed attacks by encapsulating and tunneling routing requests. Therefore, it does not seem possible to capture or model out Sybil and wormhole attacks from pure-protocol-based security models. The purpose of routing being to establish a communication infrastructure, it is always reasonable to assume the existence of alternative communication channels, namely those that route discovery will establish. Even though it is not possible to discover secure routes in general MANETs, there are several other approaches that could be used to establish secure communication channels. In the following, we consider two such approaches: multipath routes and route discovery with traceability.

XXVI. Multipath and Sub graphs

Routes need not be restricted to paths in the network graph G : Any sub graph G_{ST} of that links the source S to the target T can be used for communication. Particular interest, from a security point of view, are sub graphs G_{ST} with multiple connectivity between S ; T , for example, multipaths. Such routes may have sufficient redundancy to guarantee communication, i.e., may contain at least one secure path (with no adversarial nodes). However, there are ways to partly mitigate this. For example, the source can select communication paths in G_{ST} on a rotation basis (adaptive multipath routing). Another approach is to use random sub graphs G_{ST} of G that link S ; T . Gossip protocols use this approach, which guarantees packet propagation while minimizing the number of nodes that forward packets. The latter approach completely blurs all separation of the routing discovery, maintenance, and data communication phases. Paradoxically, this approach's meshing of functionalities may facilitate showing the compensability of its security properties.

XXVII. Route Discovery with Traceability

In general solutions such as those proposed above are only appropriate for applications in which security is critical. Perhaps, a more practical solution would be to use routing Algorithms that trace malicious behavior. It is possible to do this in such a way that there is practically no additional cost when the adversary is passive, while the extra cost is only for tracing adversarial nodes (optimistic tracing). This approach supports self-healing security: The power of the

adversary is diminished with each attack if we assume that the number of adversarial nodes is bounded over time.

XXVIII. EXPERIMENTAL RESULTS:

ADAIRNE

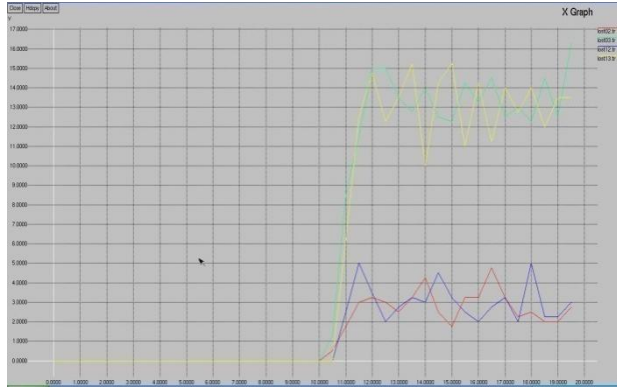


Fig.6 Loss graph



Fig.7 Throughput graph

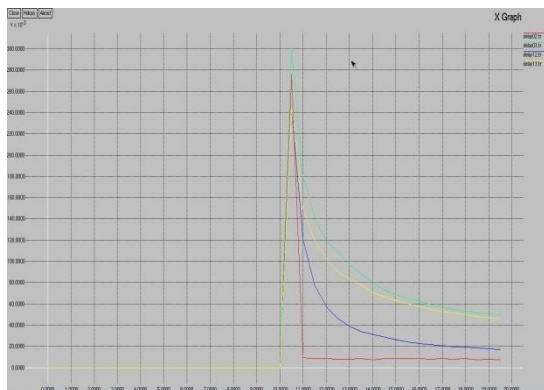


Fig.8 Delay graph

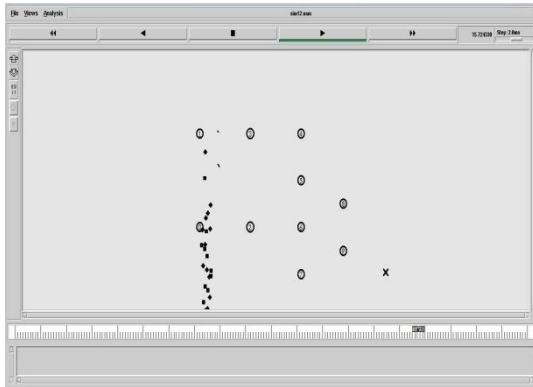


Fig.9 Adairne output

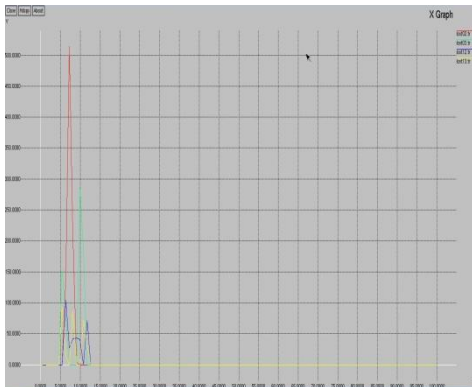


Fig.10 Loss graph

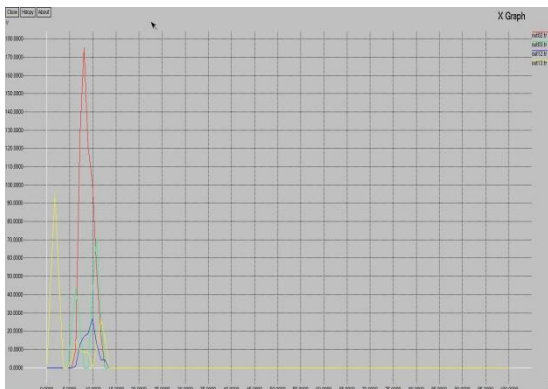
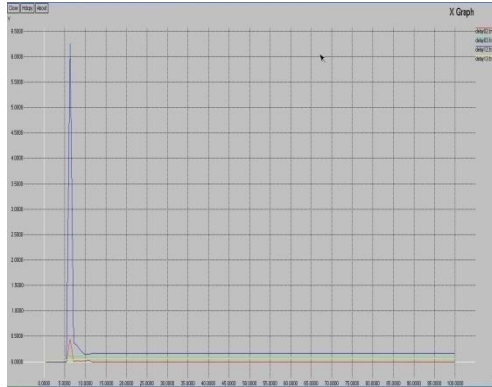
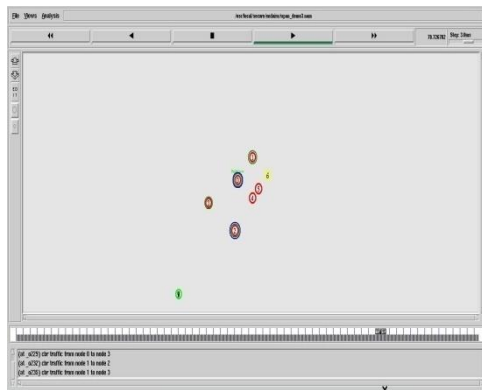


Fig.11 Throughput graph

Secure route discovery for dynamic source routing in manets

**Fig.12 Delay graph****Fig.13 EndairA output**

XXIX. ENDAIRA

The delay also shows the comparison between ARIADNE and ENDAIRA as shown in figure 13. ARIADNE (shown in fig 9) contributes higher delay than ENDAIRA. Communications, assigning MAC authentications between nodes takes more time to verify even though each node can't detect the presence of an adversary. Once the message arrives at the destination, and gets a reply back with the routes which do not exist, it will cause a problem especially when to verify the correct route after an adversary has been detected. No one will confess which one is the correct route along the transmission. The system throughput or aggregate throughput is the sum of the data rates that are delivered to all terminals in a network shown in fig 7. The throughput of a communication system may be affected by various factors, including the limitations of underlying analog physical medium, available processing power of the system components, and end-user behavior. When various protocol overheads are taken into account, the useful rate of the transferred data can be significantly lower than the maximum achievable throughput; the useful

part is usually referred to as good put shown in fig 11..Packet loss can reduce throughput for a given sender, whether unintentionally due to network malfunction, or intentionally as a means to balance available bandwidth between multiple senders when a given router or network link reaches nears its maximum capacity. When reliable delivery is necessary, packet loss increases latency due to additional time needed for retransmission. Assuming no retransmission, packets experiencing the worst delays might be preferentially dropped resulting in lower latency overall at the price of data loss shown in fig 6. During typical network congestion, not all packets in a stream are dropped. This means that un dropped packets will arrive with low latency compared to retransmitted packets, which arrive with high latency. Not only do the retransmitted packets have to travel part of the way twice, but the sender will not realize the packet has been dropped until it either fails to receive acknowledgement of receipt in the expected order, or fails to receive acknowledgement for a long enough time that it assumes the packet has been dropped as opposed to merely delayed shown in fig 10.And their corresponding delay shown in fig8&12.

XXX. CONCLUSION

A new security framework tailored for on-demand route discovery protocols in MANETs was proposed in this represents a first effort toward a formal security model that can deal with concurrent attacks and is successful in mitigating a class of hidden channel attacks the attacks that are intrinsic to the wireless broadcast medium in a neighborhood. However, as we observed above, there are a plethora of other hidden channels that become available through concurrent execution of route discovery protocols. Additionally, in the context of mobility, which requires that route discovery take place simultaneously with data communication, large additional bandwidth is naturally generated and available to adversarial nodes. Consequently, in the proposed formal model, it is impossible to prevent that adversarial nodes break up routes by inserting non existing links. To address this shortcoming, either more flexible definitions of routes must be employed (e.g., redundant routing) or it becomes necessary to address global threats directly, such as those posed by Sybil, wormhole, and more generally, man-in-the-middle attacks.

REFERENCES

- [1] Aizat Azmi, Ahmad Amsyar Azman, Sallehuddin Ibrahim, and Mohd Amri Md Yunus, "Techniques In Advancing The Capabilities Of Various Nitrate Detection Methods: A Review", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 223-261.
- [2] Tsugunosuke Sakai, Haruya Tamaki, Yosuke Ota, Ryohei Egusa, Shigenori Inagaki, Fusako Kusunoki, Masanori Sugimoto, Hiroshi Mizoguchi, "Eda-Based Estimation Of Visual Attention By Observation Of Eye Blink Frequency", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 296-307.
- [3] Ismail Ben Abdallah, Yassine Bouteraa, and Chokri Rekik , "Design And Development Of 3d Printed Myoelectric Robotic Exoskeleton For Hand Rehabilitation", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 341-366.
- [4] S. H. Teay, C. Batunlu and A. Albarbar, "Smart Sensing System For Enhanceing The Reliability Of Power Electronic Devices Used In Wind Turbines", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 2, June 2017, pp. 407- 424
- [5] SCihan Gercek, Djilali Kourtiche, Mustapha Nadi, Isabelle Magne, Pierre Schmitt, Martine Souques and Patrice Roth, "An In Vitro Cost-Effective Test Bench For Active Cardiac Implants, Reproducing Human Exposure To Electric Fields 50/60 Hz", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 1- 17
- [6] P. Visconti, P. Primiceri, R. de Fazio and A. Lay Ekuakille, "A Solar-Powered White Led-Based Uv-Vis Spectrophotometric System Managed By Pc For Air Pollution Detection In Faraway And Unfriendly Locations", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 18- 49
- [7] Samarendra Nath Sur, Rabindranath Bera and Bansibadan Maji, "Feedback Equalizer For Vehicular Channel", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 50- 68
- [8] Yen-Hong A. Chen, Kai-Jan Lin and Yu-Chu M. Li, "Assessment To Effectiveness Of The New Early Streamer Emission Lightning Protection System", International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 108- 123
- [9] Iman Heidarpour Shahrezaei, Morteza Kazerooni and Mohsen Fallah, "A Total Quality Assessment Solution For Synthetic Aperture Radar Nlrm Waveform Generation And Evaluation

In A Complex Random Media”, International Journal on Smart Sensing and Intelligent Systems., VOL. 10, NO. 1, March 2017, pp. 174- 198

[10] P. Visconti ,R.Ferri, M.Pucciarelli and E.Venere, “Development And Characterization Of A Solar-Based Energy Harvesting And Power Management System For A Wsn Node Applied To Optimized Goods Transport And Storage”, International Journal on Smart Sensing and Intelligent Systems., VOL. 9, NO. 4, December 2016 , pp. 1637- 1667

[11] YoumeiSong,Jianbo Li, Chenglong Li, Fushu Wang, “Social Popularity Based Routing In Delay Tolerant Networks”, International Journal on Smart Sensing and Intelligent Systems., VOL. 9, NO. 4, December 2016 , pp. 1687- 1709

[12] Seifeddine Ben Warrad and OlfaBoubaker, “Full Order Unknown Inputs Observer For Multiple Time-Delay Systems”, International Journal on Smart Sensing and Intelligent Systems., VOL. 9, NO. 4, December 2016 , pp. 1750- 1775

[13] Rajesh, M., and J. M. Gnanasekar. "Path observation-based physical routing protocol for wireless ad hoc networks." International Journal of Wireless and Mobile Computing 11.3 (2016): 244-257.

[14]. Rajesh, M., and J. M. Gnanasekar. "Congestion control in heterogeneous wireless ad hoc network using FRCC." Australian Journal of Basic and Applied Sciences 9.7 (2015): 698-702.

[15]. Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Ad hoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.

[16]. Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL USING AODV PROTOCOL SCHEME FOR WIRELESS AD-HOC NETWORK." Advances in Computer Science and Engineering 16.1/2 (2016): 19.

[17]. Rajesh, M., and J. M. Gnanasekar. "An optimized congestion control and error management system for OCCEM." International Journal of Advanced Research in IT and Engineering 4.4 (2015): 1-10.

[18]. Rajesh, M., and J. M. Gnanasekar. "Constructing Well-Organized Wireless Sensor Networks with Low-Level Identification." World Engineering & Applied Sciences Journal 7.1 (2016).

[19] L. Jamal, M. Shamsujjoha, and H. M. Hasan Babu, “Design of optimal reversible carry look-ahead adder with optimal garbage and quantum cost,” International Journal of Engineering and Technology, vol. 2, pp. 44–50, 2012.

- [20] S. N. Mahammad and K. Veezhinathan, “Constructing online testable circuits using reversible logic,” IEEE Transactions on Instrumentation and Measurement, vol. 59, pp. 101–109, 2010.
- [21] W. N. N. Hung, X. Song, G. Yang, J. Yang, and M. A. Perkowski, “Optimal synthesis of multiple output boolean functions using a set of quantum gates by symbolic reachability analysis,” IEEE Trans. on CAD of Integrated Circuits and Systems, vol. 25, no. 9, pp. 1652–1663, 2006.
- [22] F. Sharmin, M. M. A. Polash, M. Shamsujjoha, L. Jamal, and H. M. Hasan Babu, “Design of a compact reversible random access memory,” in 4th IEEE International Conference on Computer Science and Information Technology, vol. 10, june 2011, pp. 103–107.
- [23] Dr. AntoBennet, M, Sankar Babu G, Suresh R, Mohammed Sulaiman S, Sheriff M, Janakiraman G ,Natarajan S, “Design & Testing of Tcam Faults Using T_H Algorithm”, Middle-East Journal of Scientific Research 23(08): 1921-1929, August 2015 .
- [24] Dr. AntoBennet, M “Power Optimization Techniques for sequential elements using pulse triggered flipflops”, International Journal of Computer & Modern Technology , Issue 01 ,Volume01 ,pp 29-40, June 2015.