A SECURE SOURCE ROUTING PROTOCOL FOR AUTONOMOUS MOBILE MESH NETWORKS

[1]T.Sudha, [2]S. Ramani

[1]Research Scholar,Department of Electronics and Communication Engineering, varuvanvadivelan institute of Technology, Dharmapuri.

[2]Research Scholar, Department of Electronics and Communication Engineering, Anna University of Technology, Coimbatore.

[1]sudhainnov@gmail.com, [2] ramaniphd123@gmail.com.

Abstract: Mobile ad hoc networks (MANETs) are ideal for situations where a fixed infrastructure is unavailable or infeasible. Today's MANETs, however, may suffer from network partitioning. This limitation makes MANETs unsuitable for applications such as crisis management and battlefield communications, in which team members might need to work in groups scattered in the application terrain. In such applications, intergroup communication is crucial to the team collaboration. To address this weakness introduce in this paper a new class of ad-hoc network called Autonomous Mobile Mesh Network (AMMNET). Unlike conventional mesh networks, the mobile mesh nodes of an AMMNET are capable of following the mesh clients in the application terrain, and organizing themselves into a suitable network topology to ensure good connectivity for both intra- and intergroup communications. Here propose a distributed client tracking solution to deal with the dynamic nature of client mobility, and present techniques for dynamic topology adaptation in accordance with the mobility pattern of the clients. Our simulation results indicate that AMMNET is robust against network partitioning and capable of providing high relay throughput for the mobile clients.

1. INTRODUCTION

Mobile computing is human computer interaction by which a computer is expected to be transported during normal usage. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications.

One great challenge in designing robust MANETs is to minimize network partitions. As autonomous mobile users move about in a MANET, the network topology may change rapidly and unpredictably over time; and portions of the network may intermittently become partitioned. This condition is undesirable, particularly for mission-critical applications such as crisis management and battlefield communications. AMMNET is a good candidate because it can adapt to a very dynamic environment. Delay tolerant network (DTN) is another option to support opportunistic communications for mobile networks. However, there is no guarantee of finding a routing path to forward data. In contrast, the goal of our design is to provide such mobile networks a robust infrastructure with persistent connectivity. That if the number of mesh nodes in AMMNET is not enough to support full connectivity for the entire terrain, DTN can be used to improve the probability of data delivery leave the integration of AMMNET and DTN as our future study.

Here assume that each mobile mesh node is equipped with a localization device such as GPS. In addition, a mobile mesh node can detect mesh clients within its sensing range, but does not know their exact locations. For instance, this can be achieved by detecting beacon messages transmitted from the clients. Alternatively, RFID has been proposed for location-based applications. Similarly, mesh clients can be tagged with an inexpensive RFID and mobile mesh nodes are equipped with an RFID reader to detect the presence of mobile nodes within their sensing range.Our challenges in designing the proposed AMMNET are twofold. First, the mesh clients do not have knowledge of their

locations making it difficult for the mobile mesh nodes to synthesize a global map of the user locations. Second, the topology adaptation needs to be based on a highly efficient distributed computing technique to keep up with the dynamic movement of the mobile users.

2. RELATED WORK

A Delay-Tolerant Network Architecture for Challenged Internets propose a network architecture and application interface structured around optionally-reliable asynchronous message forwarding, with limited expectations of end-to-end connectivity and node resources.The Selection algorithm and Recovery algorithms. The DTN architecture aims to address the desire to provide interoperable
communications between and among a wide range of networks which may have exceptionally poor and disparate performance characteristics. The architecture represents a generalization of the Interplanetary Internet architecture to challenged networks other than space. The disadvantage of the proxy approach is in its specificity. Proxies usually use one of two approaches: they respond to a specialized set of commands, or act merely as raw data connectors. The first approach limits the ability to re-use the proxies. The second method fails to take advantage of any special resources the proxy node may have to offer (such as memory or processing capabilities), and requires applications communicating with the proxy to employ specialized code on a per-network basis.

ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks Propose ARSA, an attack-resilient security architecture for WMNs. In contrast to a conventional cellular-like solution, ARSA eliminates the need for establishing bilateral roaming agreements and having real-time interactions between potentially numerous WMN operators. The Symmetric-key algorithm is used. WMNs include low deployment costs, self-configuration and self-maintenance, good scalability, high robustness, and so on. Mesh clients see the advantage of being able to get on-demand network access by any WMN operator. One significant advantage of WMNs over wireless LANs lies in the multihop communication paradigm extending the network coverage. ARSA provides efficient mutual AKA not only between a user and a serving WMN domain but also between users served by the same WMN domain. In addition, it is designed to be resistant to various attacks against WMN access.

Securing Wireless Mesh Networks WMN is distinct from manets in that it uses multiple radios and relies on a high-speed back-haul network itself, often wireless that optimizes network performance and provides gateways to the wired Internet and other wireless services.Model-checking techniques and Implementation techniques are used.The advantages of this approach are that it requires only minor changes to the MAC protocol and that it can work with standard hardware.Alternative authentication protocols that are lightweight and do not place restrictions on mesh formation remain an area.The experience of the Comminus protocol shows this is possible but underscores the importance of rigorous validation.

A Structured Group Mobility Model for the Simulation of Mobile Ad Hoc Networks This paper presents the Structured Group Mobility Model (SGMM), which parameterizes group structure and generates movement sequences for use in simulations. The Routing algorithms are used.The advantage that it allows a user to accurately describe the real-world behavior of groups with inherent structure.This paper presents a study of real-world group movement scenarios for mobile ad hoc networks.Groups in real-world MANET scenarios exhibit internal structure.A mobility model that captures structure inherent in groups produces different results than those that do not capture structure will continue to refine the SGMM with an eye toward broadening its application. In particular although described four real-world scenarios where groups move with internal structure have only simulated hierarchical military vehicle movements.Approximation Algorithms for Partial Covering Problems obtain a polynomial-time approximation scheme for k-partial vertex cover on planar graphs, and for covering k points in Rd by disks. The Approximation Algorithms and Set cover algorithm are used. It presented improved approximation algorithms for a family of partial covering problems. Upon these ideas and by employing semi definite programming. It has been shown that partial vertex cover in graphs with maximum degree d, can be approximated.

R-Trees. A Dynamic Index Structure For Spatial

Searching present the results of a series of tests which indicate that the structure performs well, and conclude that it is useful for current database systems m spatial applications. Search algorithm, Insert algorithm and Deletion algorithm are used. The linear node-split algorithm proved to be as good as more expensive techniques. It was fast] and the slightly worse quality of the splits did not affect search performance noticeably. Preliminary investigation indicates that R-trees would be easy to add to any relational database system that supported conventional access methods. Structure would work especially well in conjunction with abstract data types and abstract modules to streamline the handling of spatial data.

Some Methods for Classification and Analysis of Multivariate Observations The k-means concept represents a generalization of the ordinary sample mean, and one is naturally led to study the pertinent asymptotic behavior, the object being to establish some sort of law of large numbers for the k-means. The K-means clustering algorithm is used. Numerous classifications cheaply and thereby look at the data from a variety of different perspectives is an important advantage. Another general feature of the k-means procedure which is to be expected on intuitive grounds and has been noted in practice is a tendency for the means and the associated partition to avoid having the extreme of only one or two points in a set.

Convergent subsequences of the sequence of sample k-centroids will have their limits in the class of unbiased k points. Certain difficulties encountered in the proof of theorem 1 are caused by the possibility of the limit of a convergent sequence of k-points having some of its constituent points equal to each other.Clustering by Passing Messages Between Data Points Clustering data by identifying a subset of representative examples is important for processing sensory signals and detecting patterns in data. The Max-sum algorithm and Expectation maximization (EM) algorithm One advantage of affinity propagation is that the number of exemplars need not be specified beforehand. Affinity propagation has several advantages over related techniques. Methods such as k-centers clustering K-means clustering and the expectation maximization (EM) algorithm store a relatively small set of estimated cluster centers at each step. Understanding their limits is a main open challenge.At the lowest level this means controlling the convergence properties or the quality of the approximate solutions that they find. A more ambitious goal is to characterize the problems where they can be useful.

Wireless mesh networks: a survey WMNs are anticipated to resolve the limitations and to significantly improve the performance of ad hoc networks, wireless local area networks (WLANs), wireless personal area networks (WPANs) and wireless metropolitan area networks (WMANs). They are undergoing rapid progress and inspiring numerous deployments. The Sophisticated algorithms and Topology control algorithms. The analysis is simplified by taking advantage of the low mobility feature of WMNs. The advantages brought by such physical layer techniques will be significantly compromised. Despite its advantages, an entirely new transport protocol is not favored by WMNs due to the compatibility issue. WMNs will lose the autonomic feature. However, current WMNs can only partially realize this objective. Current security approaches may be effective to a particular attack in a specific protocol layer, but lack a comprehensive mechanism to prevent or counter attacks in different protocol layers.

Comparison of Routing Metrics for Static Multi-Hop Wireless NetworksA routing algorithm can select better paths by explicitly taking the quality of the wireless links into account. The Routing algorithm and Link-MaxLife algorithm. Their implementation takes advantage of 802.11 link-layer acknowledgments for failure detection. The primary advantage of this metric is its simplicity. Once the topology is known, it is easy to compute and minimize the hop count between a source and a destination. The primary disadvantage of this metric is that it does not take packet loss or bandwidth into account. There is the overhead of measuring the round trip time. Reduce this overhead by using small probe packets (137 bytes). The metric doesn't explicitly take link data rate into account.

3. PROPOSED APPROACH

Address this challenging problem by proposing a new class of robust mobile ad hoc network called AMMNET. To maintain the communication between all nodes even they are in different groups Mesh Nodes

are used. Mesh Nodes which have the capability of changing its nature into Inter-group router or Intra-group router even it can act as a bridge router. To make the communication effective One-hop neighbor information update is used to find the shortest path between any two nodes.

The conventional mobile ad-hoc network suffer from network partitioning, this problem was solved in the AMMNET. It supports both intra-routing and inter-routing. Here the mobile mesh routers of an AMMNET track the users and dynamically adapt the Network topology and perform routing. It simply forwards the date from source to destination via multiple hops. This infrastructure provides full connectivity without need of high cost of network coverage. AMMNET does not consider that whether the routing path is the one which is shortest distance between the source-destination pair. Therefore one-hop neighbor information update method used to find the shortest route. It maintains the information's such as location, ID, distance and mobility of its neighbors and provides cost-effective solution. To provide security here using secure crypto Algorithm.

SYSTEM ARCHITECTURE

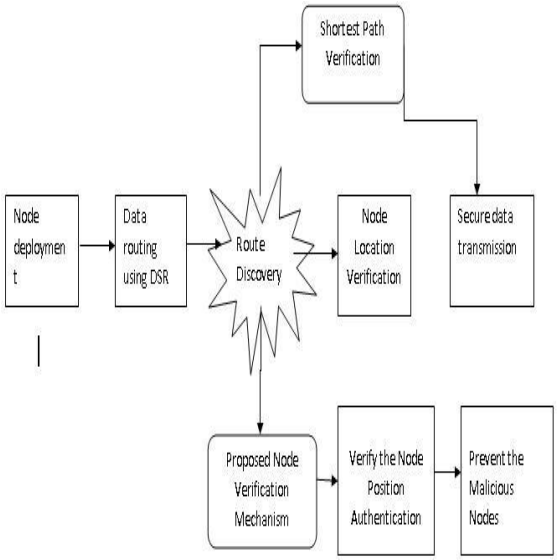

Figure 1: Architecture Diagram

4. PROPOSED APPROACH

- NODECONFIGURATUION SETTING
- NODES UNIQUE IDENTITY
- MESSAGE EXCHANGE PROCESS FOR ROUTE DISCOVERY
- DISTANCE COMPUTATION
- NODE POSISTION VERIFICATION
- NODE VERIFICATION PROCESS
- GRAPH EXAMINATION

4.1 Project Description

- **Node configuratuion setting**

The mobile nodes are designed and configured dynamically, designed to employ across the network, the nodes are set according to the X, Y, Z dimension, which the nodes have the direct transmission range to all other nodes.

- **Nodes Unique Identity**

All the mobile nodes tend to have a unique id for its identification process, since the mobile nodes communicates with other nodes through its own network id. If any mobile node opted out of the network then the particular node should surrender its network id to the head node.

- **Message Exchange Process For Route Discovery**

This module states a 4 step message exchange process i,e POLL, REPLY, REVEAL, REPORT. As soon the protocol executed the, POLL and REPLY messages are first broadcasted by Source and its neighbors, respectively. These messages are anonymous and take advantage of the broadcast nature of the wireless medium, allowing nodes to record reciprocal timing information without disclosing their identities.

- **Distance Computation**

In order to compute the distance range, after a POLL and REPLY message a REVEmessage broadcast by the source nodes disclose to S, through secure and authenticated REPORT messages, their identities as well as the anonymous timing information they collected. The source S uses such data to match timings

and identities; then, it uses the timings to perform ToF-based ranging and compute distances between all pairs of communicating nodes in its neighborhood.

- **Node Posistion Verification**

Once Source node has derived such distances, it runs several position verification tests in order to classify each candidate neighbor as either: Verified node, i.e., a node the verifier deems to be at the claimed position or Faulty node, i.e., a node the verifier deems to have announced an incorrect position or Unverifiable node, i.e., a node the verifier cannot prove to be either correct or faulty, due to insufficient information. The position verification is performed by direct symmetric test, cross symmetry test and multilateration test.

- **Node Verification Process**

In this module a proposed work of node verification technique is introduced to detect the adversary nodes in the network. The node verification is done by hash function technique the public key and id of source node generates hash id. In the same way the neighbor nodes generate the hash id, if the source node hash id and neighbor node hash id are same then the nodes are authenticated for data transmission through the minimum distance range discovered path to destination.

- **Graph Examination**

The performance analysis of the existing and proposed work is examined through graphical analysis.

- **Techniques And Algorithm**

Crypto Algorithm

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The key management process used for cryptography application during data transfer.The cryptography technique used to product the node and data from different kind of attacks.

Here use the node forwarding mechanism for key management. The acknowledgment service provide the ensure the data transfer. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems such as the RSA algorithm are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is Infeasible.

The size of the elliptic curve determines the difficulty of the problem. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements. For current cryptographic purposes an elliptic curve is a plane curve which consists of the points satisfying the equation more complicated.

$$y2=x3+ax+b$$

This set together with the group operationof the elliptic group theory form an Abelian group with thepoint at infinity as identity element. The structure of the groupis inherited from the divisor group of the underlying algebraicvariety. How it works depends on the cryptographic schemeyou apply it to. As an example, it can be applied it to theDiffie-Hellman key exchange, which is commonly known asthe Elliptic Curve Diffie-Hellman (ECDH) key agreementprotocol. Suppose Alice wants to establish a shared key with Bob but the only channel available for them may be eavesdropped by a third party. Initially, the domain parameters (that is, (p,a,b,G,n,h) in the prime case or (m,f(x),a,b,G,n,h) in the binary case) must be agreed upon. Also, each party must have a key pair suitable for elliptic curve cryptography, consisting of a private key d (a randomly selected integer in the interval [1,n−1]) and a public key Q (where Q=dG). Let Alice's key pair be (dA,QA) and Bob's key pair be (dB,QB). Each party must have the other party's public key (an exchange must occur). Alice computes (xk,yk)=dAQB. Bob computes k=dBQA. The shared key is xk (the x coordinates of the point).

- **Route Maintenance**

As it is an on-demand routing protocol so it looks up the routing during transmission of a packet. At the first phase the transmitting node search its route cache to see whether there is a valid destination exists and if so then

the node starts transmitting to the destination node and the route discovery process end here. If there is no destination address then the node broadcasts the route request packet to reach the destination.

When the destination node gets this packet it returns the learned path to the source node. The route discovery process involves sending route-request packets from a source to its neighbor nodes which then forward the request to their neighbors and so on.

Once the route-request reaches the destination node it responds by unicasting a route reply packet back to the source node via the neighbor from which it first received the route request. When the route request reaches an intermediate node that has a sufficiently up-to-date route it stops forwarding and sends a route-reply message back to the source. Once the route is established some form of route maintenance process maintains it in each node's internal data structure called a route-cache until the destination becomes inaccessible along the route.

- **Trunk status map routing (TSMR)**

DNHR (Dynamic nonhierarchical routing)measures traffic once a week.

TSMR updates measurements once an hour or so only if it changes "significantly".

List of alternative paths is more up to date.

- **Tracking Mechanism**

A client can connect to any nearby mesh node which helps relay data to the destination mesh node via multihop forwarding. To support dynamically changing mesh topology mobile mesh nodes can be classified into three types.

i) Intergroup routers.

ii) Intra-group routers.

iii) Free routers.

The intergroup routers perform routing between the groups the intra-group routers perform routing inside the group and redundant routers claimed as free routers. The low power node is replaced as a free router and can go back to the initial location for example control center to replace the battery.

Adapting to Intra-group Movement Sometimes the client c moves out of the communication range of router r into the communication range of an adjacent router r1 in the same group the another possible scenario also can occur (i.e.) the missing client c moves from the communication range of router r to a space not currently covered by any of the routers in the group.

- **Reclaiming Redundant Routers**

If intra- and intergroup routers are no longer required due to client mobility the AMMNET should reclaim them. If the all clients of router r are covered by neighboring routers r can switch to become an intergroup router.

- **Interconnecting Groups**

Given a set of intra-group routers that provide communication coverage for a group of mobile users these mobile users might move out of this coverage area in smaller groups. To avoid network partitioning each of the new groups must be supported by their local intra group routers and intergroup routers must organize themselves into a sub-network of bridges to support the intergroup communications.

- **Routing Protocol**

There are two different types of protocol.

- **Table-Driven (Proactive)**

The nodes maintain a table of routes to every destination in the network for this reason they periodically exchange messages. Keeping routes to all destinations up-to-date even if they are not used is a disadvantage with regard to the usage of bandwidth and of network resources.

- **On-Demand (Reactive)**

These protocols were designed to overcome the wasted effort in maintaining unused routes. Routing information is acquired only when there is a need for it. The needed routes are calculated on demand. This saves the overhead of maintaining unused routes at each node but on the other hand the latency for sending data packets will considerably increase. These protocols were designed to overcome the wasted effort in

maintaining unused routes. Routing information is acquired only when there is a need for it.

- **One-hop neighbor information update**

To make the communication effective One-hop neighbor information update is used to find the shortest path between any two nodes. For communication between the nodes or between groups initially the source enables the route discovery process to find the shortest path based on one hop neighbor information. All the nodes in network maintain information such as location, ID, distance and mobility of its neighbors. Based on this information, source finds the shortest path to communicate with destination. Shortest path also contains minimum number of intermediate hops.

- **Algorithm**

Step 1: Nodes share and store information (id, position, distance, mobility) of its neighbors who are in closer than others in its coverage range.
Step 2: Source enables route discovery process. While receiving discovery packet each node forwards to its one hop neighbors.
Step 3: source receives acknowledgement (intermediate hop ids, distance) from intermediate hops (relays) and destination.
Step 4: source finds shortest path by received acknowledgement from destination.
Step 5: Sends data through that path.

- **Communication in single group**

When the nodes in the single group the intra-group router used for routing. This communication is performed inside the group.

- **Intra-routing**

To perform communication between the groups the inter group routers and bridge routers are used. Here the major constraint is distance. In the small distance communication the inter router used whereas in case of long distance communication the bridge router used. The following simulation results indicate the difference between those situations.

- **Performance of Network Coverage**

Each simulation includes 50 clients classified into three mobile groups. Vary the moving speed of routers from the mean speed of clients to six times of the mean speed of clients. Oracle always uses the up-to-date location information of clients to re-compute the topology and thereby can best utilize all available routers. Some failures occur under AMMNET due to tracking of clients. In AMMNET global adaptation cannot be performed all the time therefore it requires more routers to cover all the clients compare to Global-AMMNET. Whereas Oracle connects every client using an R-tree with more layers as compared to the R-tree only including bridge routers in AMMNET might require a few more routers to cover the entire hierarchical topology.

5. CONCLUSION

The proposed work conducted extensive simulation study to assess the effectiveness of AMMNET. The results confirm that the proposed distributed topology adaptation scheme based on autonomous mobile mesh routers is almost as effective as a hypothetical centralized technique with complete knowledge of the locations of the mobile clients. The simulation results also indicate that AMMNET is scalable with the number of users.

6. FUTURE WORK

Although an excessively large number of user groups may affect the performance of AMMNET, the number of user groups is typically very small relative to the number of users for most applications and AMMNET is effective for most practical scenarios. There are still many interesting issues not yet examined in our study such as searching for disappearing mobile clients, minimizing routing paths, and utilizing non-overlapping channels leave these changes for future research.

REFERENCES

[1] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Proc. ACM Special Interest Group on Data Comm., 2003

[2] Y. Zhang and Y. Fang, "ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 10, pp. 1916-1928, Oct. 2006.

[3] J. Sun, C. Zhang, and Y. Fang, "A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks," Proc. IEEE INFOCOM, 2008.

[4] B. Salem and J. Hubaux, "Securing Wireless Mesh Networks," IEEE Wireless Comm., vol. 13, no. 2, pp. 50-55, Apr. 2006.

[5] R. Gandhi, S. Khuller, and A. Srinivasan, "Approximation Algorithms for Partial Covering Problems," Proc. 28th Int'l Colloquium Automata, Languages and Programming, pp. 225-236, 2001

[6] A. Guttman, "R-Trees: A Dynamic Index Structure for Spatial Searching," Proc. ACM SIGMOD Int'l Conf. Management of Data (SIGMOD), 1984.

[7] J. MacQuene, "Some Methods for Classification and Analysis of Multivariate Observations," Proc. Fifth Berkeley Symp. Math. Statistics and Probability, 1964

[8] B. Frey and D. Bueck, "Clusterin by Passing Messages between Data Points," Science, vol. 315, no. 5814, pp. 972-976, 2007.