Volume 2, No. 1, Jan-Feb 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

An Application Based Routing Protocol for Mobile Ad-hoc Network

Vismay Jain
Department of C.S.E.
Samrat Ashok Technological Institute
Vidisha, M.P., India
jain.vismay3@gmail.com

Abstract: A wireless ad hoc network is a collection of two or more devices/nodes or terminals with wireless communications and networking capability that communicate with each other without the aid of any centralized administrator. They do not have a fixed topology or infrastructure hence they are also known as infrastructureless networks. Each node in a wireless ad hoc network functions as a host or a router or both. The network topology is in general dynamic and the communication is via an open medium, which is vulnerable. We consider a routing protocol, namely, Dynamic Source Routing (DSR). The DSR is an on-demand or reactive routing protocol based on the concept of source routing. In this thesis a cryptographic algorithm is used in order to secure the MANETs. The cryptography is a concept inspired from the field of life science and has been extended to the field of MANETs to secure them. In the present work, one potential key application is used for cryptography systems because it provides a much more compact storage medium. The proposed routing protocol has been verified and validated through various simulation scenarios, using synthetically generated data sets. Simulation results demonstrate that the algorithm is secure with marginal overhead.

Keywords- MANET, Routing Protocols, Cryptography.

I. INTRODUCTION

With recent advances in mobile technology and mobile devices, mobile computing has become
an important part of our life. People are using wireless networks for their day-to-day work, be it making a phone call or to download news or to see and listen or only listen to their favorite song from various multimedia servers with the help of various devices such as mobile phones, PDAs or a laptop. More services are in the offering in near future. The desire to be connected *anytime, anywhere, anyhow* has led to the development of wireless networks, opening new vista of research in pervasive and ubiquitous computing. This emerging field of mobile and nomadic computing requires a highly secure routing protocol to effectively manage the communication among the peers [1] and [2].

Wireless networks, in general, refer to the use of infrared or radio frequency signals to share information and resources between devices. Due to basic difference in the physical layer (ISO/OSI model, the wireless devices and networks show distinct characteristics from their wireline counterparts, such as:

[a] Higher interference results in lower reliability.
[b] Low bandwidth and much slower data transfer rate.
[c] Highly variable network conditions.
[d] Limited computing and energy resources.
[e] Device size limitation, and
[f] Weaker security.

Apart from these limitations the wireless networks are immensely popular because of the benefits of using wireless technologies, such as:

A. Access to more than one technology –

Users can use more than one access technology to service various parts of their network and during the migration phase of their networks, when upgrading occurs on a scheduled basis. It enables a fully comprehensive access technology portfolio to work with existing technologies.

B. Minimal cost –

The inherent nature of wireless is that it doesn't require wires or lines to accommodate the data/voice/video pipeline. Although paying fees for access to elevated areas such as masts, towers, and building tops is not unusual but the associated logistics, and contractual agreements are often minimal as compared to the costs of trenching a cable.

C. Reduced time to revenue –

Companies can generate revenue in less time through the deployment of wireless solutions than with comparable access technologies because a wireless system can be assembled and brought online in a very short span of time.

D. Provides broadband access extension –

Wireless commonly competes and complements existing broadband access. Wireless technologies play a key role in extending the reach of cable, fiber, and Digital Subscriber Link (DSL) markets, and it does so quickly and reliably [2] and [5].

II. BACKGROUND

Mobile computing is proliferating as devices are becoming smaller, cheaper, and more powerful. By combining mobile devices with wireless communication abilities, the vision of being connected *anytime, anywhere, anyhow* will soon be a reality. New applications arise from mobile entities interacting and collaborating towards a common goal. With cellular phones being widely employed and the mobile Internet emerging into the market place, concepts of dynamic wireless networks that do not depend

on expensive infrastructure draws attention to the area of ad hoc networks. Mobile devices constitute a mobile ad hoc network when they directly and wirelessly communicate with other devices nearby without any fixed infrastructure. The mobile nodes move and thus the network topology changes dynamically and frequently. The absence of any hierarchy, established infrastructure, or centralized administration forces the nodes to control the network on their own. "A 'mobile ad hoc network' (MANET) is an autonomous system of mobile routers (and associated hosts) connected by wireless links-the union of which forms an arbitrary graph. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet". The ultimate goal of MANETs is to provide secure routing of data resources to mobile users at anytime and from anywhere. In conjunction with the existing routing protocols, providing security for MANETs give rise to significant challenges and performance opportunities [9].

A. Routing in MANETs-

A routing protocol is the mechanism by which user traffic is directed and transported through the network from the source node to the destination node. Objectives include maximizing network performance from the application point of view - application requirements- while minimizing the cost of network itself in accordance with its capacity. The application requirements are hop count, delay, throughput, loss rate, stability, jitter, cost; and the network capacity is a function of available resources that reside at each node and number of nodes in the network as well as its density, frequency of end-to-end connection (i.e. number of communication), frequency of topology changes (mobility rate). The four core basic routing functionality for mobile ad hoc networks are:

[a] Path generation: which generates paths according to the assembled and distributed state information of the network and of the application; assembling and distributing network and user traffic state information?

***[b] Path selection*:** This selects appropriate paths based on network and application state information.

***[c] Data Forwarding*:** This forwards user traffic along the select route forwarding user traffic along the selected route [1], [3] and [7].

***[d] Path Maintenance*:** maintaining of the selected route.

B. *Dynamic Source Routing (DSR) Protocol-*

Dynamic Source Routing (DSR) was developed at Carnegie Mellon University. It is a direct descendant of the source routing scheme used in bridged LANs. This protocol is designed to restrict the bandwidth consumption by control packets as it eliminates the periodic table-update by the control packets. As compared with other on-demand routing protocols, it is a *beacon-less* and therefore does not require periodic *hello* packet (*beacon)* transmission, usually used by a node to inform its presence to the neighbors. The basic approach of this protocol is briefly described as under:

The sender of a packet determines the complete sequence of nodes through which the node has travel. The sender of the packet explicitly mentions the list of all nodes in the packet's header, identifying each forwarding 'hop' by the address of the next node to which to transmit the packet on its way to destination host. In this protocol the nodes don't need to exchange the Routing table information periodically and thus reduces the bandwidth overhead in the network. Each Mobile node participating in the protocol maintains a *routing cache,* which contains the list of routes that the node has learnt. Whenever the node finds a new route it adds the new route in its routing cache. Each mobile node also maintains a sequence counter 'request id' to uniquely identify the requests generated by a mobile host. The pair < source address, request id > uniquely identifies any request in the ad hoc network. The protocol does not need transmissions between hosts to work in bi-direction. The main phases in the protocol are – Route Discovery phase and Route Maintenance phase.

C. Route Discovery Phase-

Router discovery allows any host to dynamically discover the route to any destination in the Ad Hoc network. In DSR, a source initiates a route discovery process when the source wants to send a packet to a destination to which it doesn't have a valid route. The Source, if it has the valid route in its routing cache then it uses it otherwise it sends a route request packet by broadcasting it to the neighbors. The route request packet contains the source address; request- id and a route record in which the sequence of hops traversed by the request packet before reaching the destination are noted down. A node upon getting a Route request packet does the following:

It checks to see if it has the pair <initiators address, request id> in its list of recently seen requests if so discard the packet.

[a] Otherwise, if this host's address is already present in the route record of the request packet then it discards the packet. This eliminates the looping problem.

[b] Otherwise, if the destination the source is looking for matches with its address then it sends the route reply packet to the initiator containing the list of nodes the request packet has traversed before it reached the destination.

[c] Otherwise, it appends its own address to the route request packet and rebroadcasts it. The route request travels the network until it reaches the destination node.

D. Route Maintenance Phase-

Route maintenance is a procedure of monitoring the correct operation of route in use. The host that uses the route does this maintenance. Since the nodes do not exchange any routing information in this protocol the route maintenance procedure monitors the operation of the route and informs the source of any errors. Any host if it detects that its neighboring node, which is the next hop for a route, is not working then the node sends an *error packet* containing its address and the address of the hop not working. A node upon receiving the route error packet removes the hop in error from its routing cache. Acknowledgements are used to verify the correct operation of the route. The route maintenance can be provided by using either hop-to-hop or by using end-to-end acknowledgements. In case of hop-to-hop acknowledgements the hop in error is indicated in the route error packet. But in case of end-to-end acknowledgements the source node assumes that the last hop of the route to the destination is error [4], [9] and [12].

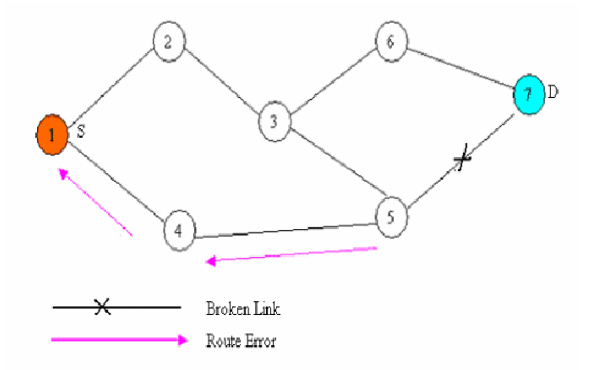


Figure-1 Route maintenance in DSR

E. Security in MANETs-

Security in a MANET is an essential component for basic network functions like packet forwarding and routing. The network operation can be easily jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. Unlike conventional networks, the ad hoc networks carry out basic support functions like - packet forwarding, routing, and network management all of the available nodes without the support of dedicated nodes and also the data travels through the open medium.

As opposed to dedicated nodes of a wired network, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions. Further, when tamper-proof hardware and strong authentication infrastructure(s) are not available, for example, in an open environment where a common authority that regulates the network does not exist, any node of an ad hoc network can endanger the reliability of basic functions like routing. The correct operation of the network requires not only the correct execution of critical network functions by each participating node but it also requires that each node perform a fair share of the functions. The latter requirement seems to be a strong limitation for wireless mobile nodes, which have to save power for their operation, so that they can 'live' on the network for a longer time period. Due to the lack of a priori trust, classical network security mechanisms based on authentication and access control cannot cope with selfishness and cooperative security schemes seem to offer the only reasonable solution. In a cooperative security scheme, node misbehavior can be detected through the collaboration between the numbers of nodes, assuming that a majority of nodes do not misbehave.

F. Active Attacks-

Active attacks are the attacks that are performed by the malicious nodes that bear some energy cost in order to perform the threat. These attacks can be classified into further following types.

[a] Impersonation: Since current ad hoc routing protocols do not *authenticate* routing packets a malicious node can launch many attacks in a network by masquerading as another node (known as *spoofing*). Spoofing occurs when a malicious node misrepresents its identity in order to alter the vision of the network topology that a benign node can gather.

[b] Modification: Existing routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Malicious nodes can easily cause traffic subversion and denial of service by simply altering the fields of the packet: such attacks compromise the *integrity* of routing computations.

[c] Fabrication: The notation "fabrication" is used when referring to attacks performed by generating false routing messages. Such kind of attacks can be difficult to identify as they come as valid routing constructs, especially in the case of fabricated routing error messages, which claim that a neighbor can no longer be contacted.

[d] Wormhole Attack: A more subtle type of active attack is the creation of a tunnel (or wormhole) in the network between two colluding malicious nodes linked through a private network connection. This exploit allows a node to short-circuit the normal flow of routing messages creating a virtual vertex cut in the network that is controlled by the two colluding attackers.

[e] Denial of Service: This active attack aims at obstructing or limiting access to a certain resource. The resource can be a specific node or service or the whole network. The nature of ad-hoc networks, where several routes exist between nodes and routes are very dynamic gives ad hoc a built-in resistance to Denial of Service attacks, compared to fixed networks [4], [6] and [7].

III. PROPOSED TECHNIQUE

The word "cryptography" is derived from Greek and when literally translated, means "secret writing." Before the advent of digital communications, cryptography was used primarily by the military for the purposes of espionage. With the advances in modern communication, technology has enabled businesses and individuals to transport information at a very low cost via public networks such as the Internet. This development comes at the cost of potentially exposing the data transmitted over such a medium. Therefore, it becomes imperative for businesses to make sure that sensitive data is transferred from one point to another in an airtight, secure manner over public networks. Cryptography can help us achieve this goal by making messages unintelligible to all but the intended recipient.

Traditionally, cryptography was a government monopoly with very little cross-fertilization between governments. The Cryptographic algorithms were designed and evaluated by government experts and details were kept secret. Governments trusted their procedures and hence trusted the cryptography. Although the cryptographic details were kept secret, this secrecy was not relied on for the security of the communications. The change over recent decades is that cryptography has become a necessary tool for a wide commercial market.

A. Cryptosystems Using Random One-Time-Pads-

One-time-pad encryption uses a codebook of random data to convert plaintext to ciphertext. Since the codebook serves as the key, if it were predictable (i.e. not random), then an adversary could guess the algorithm that generates the codebook, allowing decryption of the message. No piece of data from the codebook should ever be used more than once. If it were, then it would leak information about the probability distribution of the plaintext, which would result in increasing the efficiency of an attempt to guess the message. This class of cryptosystem using a secret random

one-time-pad is the only cryptosystem known to be absolutely unbreakable.

First, assemble a large one-time-pad in the form of a strand, which is randomly assembled from short oligonucleotide sequences, then isolated and cloned. These one-time-pads are assumed to be constructed in secret, and we further assume that specific one-time-pads is shared in advance by both the sender and receiver of the secret message. This assumption requires initial communication of the one-time-pad between sender and receiver, which is facilitated by the compact nature.

B. Cryptosystem using one-time-pad Substitution system-

A substitution one-time-pad system uses a plaintext binary message and a table defining a random mapping to ciphertext. The input strand is of length *n* and is partitioned into plaintext words of fixed length. The table maps all possible plaintext strings of a fixed length to corresponding cipher text strings, such that there is a unique reverse mapping.

Encryption by substituting each occurs plain text word with a corresponding cipher word. The mapping is implemented using a long pad consisting of many segments, each of which specifies a single plain-text word to cipher word mapping. The plaintext word acts as a hybridization site for the binding of a primer, which is then elongated. This results in the formation of a plaintextciphertext word-pair. Further, cleavage of the word-pairs and removal of the plaintext portion must occur.

The repeating unit is made up of:

[a] One sequence word, Ci, from the set of cipher or codebook-matching words;

[b] One sequence word, Pi, from the set of plaintext words; and

[c] A polymerase "stopper" sequence.

If for experimental reasons, a small lexicon is required, then the words used could represent a more basic set such as ASCII characters, resulting in a lexicon size of 128. It is estimated that in a single cloning procedure, we can produce 10^6 to 10^8 different one-time-pad sequences. It is important to note that the choice of word encodings must guarantee an acceptable Hamming distance between sequences such that the fidelity of annealing is maximized. The entire construction process can be repeated to prepare greater numbers of unique pads. Construction of the libraries of codebook pads can be approached using segmental assembly procedures used successfully in gene library construction projects and the word encoding methods used in the computation. We can set the constants C1 and C2 large enough so that the probability of getting repeated words on a pad of length *n* is acceptably small. Each of the encryption/ decryption process is performed ten times and the average time is considered and for checking the robustness of the system, we have selected four different plain texts with increasing size.

The program is designe for a simple sender-receiver system. On the sender side, an initial key is required (starting introns and pattern codes) which the user himself generates. The user first translates the plaintext into the of information using conversion program. Processes of central dogma – splicing, transcription and translation are also simulated including necessary padding for compatibility reason. Now, the starting and pattern codes of the introns along with the places of introns, removed spaced introns and the codon-amino acid are added into the key file and the enciphered information is also created. These two files are then sent to receiver through two different channels, the enciphered file through public channel and the key file through secure channel. At the receiver side, the enciphered information and the key file are received from two different channels. The key information in the key file is used to decipher the received information. Reverse translation, reverse transcription and reverse splicing processes are applied using the respective program and the information stored in the key file. After this process the receiver gets the information and then the plain text can be easily recovered in order to know what the sender has sent to the receiver. We have used highly divert plaintext, which include short-text, long-text purely alphabetical and text combining alphabets in order to test the performance of the program. Further, each plaintext has the length 10 times that of the former one, starting from 10 and then number bits needed to store in ASCII format is calculated, which is eight times the length of plain text. As observed we have also introduced the redundancies (tags and separators). The actual key information is dependent on size of the starting and pattern codes of the introns but its size is roughly less than half of the size including redundancy.

The encryption and decryption times are also listed, which points towards the efficiency of the algorithm.

C. Method Analysis-

The experimental feasibility depends upon the following factors:

[a] The size of the lexicon, which is the number of plaintext-ciphertext word-pairs,

[b] The size of each word,

[c] The number of one-time-pads that can be constructed in a synthesis cycle.

[d] The length of each message that is to be encrypted.

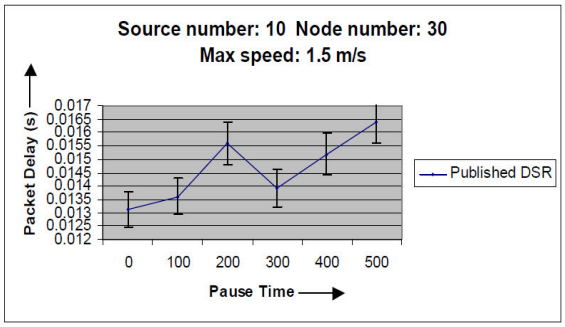
If for experimental reasons, a small lexicon is required, then the words used could represent a more basic set such as ASCII characters, resulting in a lexicon size of 128. It is estimated that in a single cloning procedure, we can produce 10^6 to 10^8 different one-time-pad sequences. It is important to note that the choice of word encodings must guarantee an acceptable Hamming distance between sequences such that the fidelity of annealing is maximized. The entire construction process can be repeated to prepare greater numbers of unique pads. Construction of the libraries of codebook pads can be approached using segmental assembly procedures used successfully in gene library construction projects and word encoding methods used in DNA computation.

We can set the constants C_1 and C_2 large enough so that the probability of getting repeated words on a pad of length *n* is acceptably small.

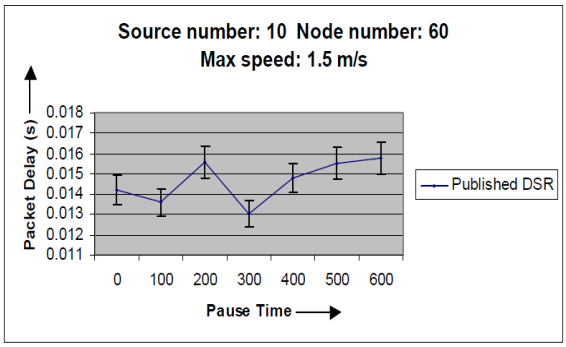
IV. RESULTS

The Route Acquisition Time overhead is increased, indicating minimal interference of the proposed protocol, with the normal functioning of the DSR protocol (3% to 4%). The End-to-End Delay overhead is increased over the DSR protocol due to the extra time required to communicate the public key and the encryption and decryption process taking place at the source and destination nodes (around

12%). A Routing Overheadoverhead increases because of the extra information being sent as encrypted message (12% to 14%). The Throughput overhead of DSR protocol is almost constant, ranging from 8% to 12.5% because the number of packets lost while reaching the destination is almost same in both the cases.

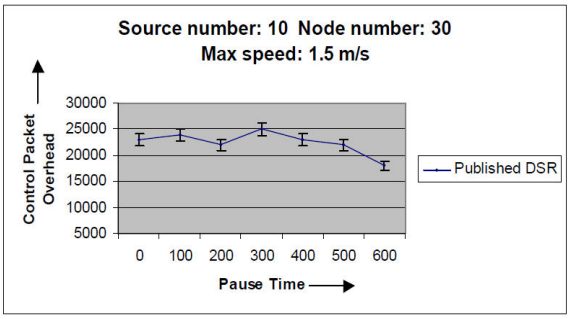


(a)

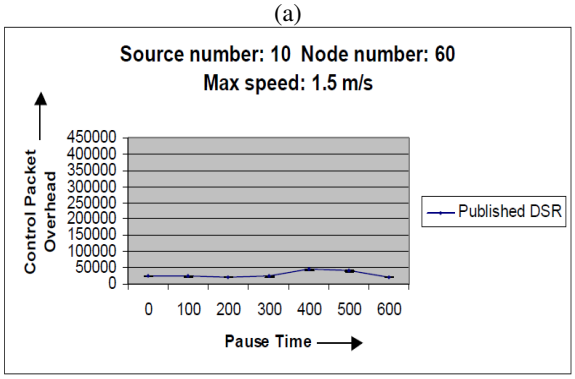


(b)

Figure- 2 Graphs showing the output of Packet Delay for Published DSR against different simulation Parameters.



(a)



(b)

Figure-3 Graphs showing the output of Routing Overhead for Published DSR against different simulation Parameters.

V. CONCLUSIONS

Wireless mobile ad hoc networks present difficult challenges to routing protocol designers. Mobility, constrained bandwidth, and limited power cause frequent topology changes. It also has its share of security vulnerabilities. The very basic nature of the mode of communication is the main concern because anything that moves over the open air medium is susceptible to be picked up by unauthorized access. For any mission critical or organizationally sensitive information, ad hoc networks add an element of insecurity. The most important and vital element is to route the information among the network in a secured manner. We conducted a performance evaluation of various routing protocols of different types, mainly focusing on the flat-routing protocols. The routing protocols were analyzed in diverse network scenario to assess their relative strength and weaknesses. Our results provided meaningful indications to protocol designers in this area. We investigated the effect of various mobility models on working of different flat-routing protocols. It is determined that the choice of mobility model does, in fact, affect the relative performance of different routing protocols. We performed simulation of the DSR protocol. Our study results indicate that DSR may be considered as one of the best routing protocol for providing secure routing because there are no periodic beacons, thus resulting in a lesser overhead during communication.

VI. REFERENCES

[1] Rashid Amin, Shehzad Ashraf ch, M Bilal Akhtar, Aftab Ahmed Khan, "Analyzing Performance of Ad hoc Network Mobility Models in a Peer-to-Peer Network Application over Mobile Ad hoc Network ", IEEE2010- Conference on Electronics and Information Engineering.

[2] A. K. Verma, Mayank Dave and R C Joshi, "Genetic Algorithm and Tabu Search Attack on the Mono-Alphabetic Substitution Cipher in Ad-hoc Networks," International J. of Computer Science, NY (USA), 3(3), 134-137, 2007.

[3] A. K. Verma, Mayank Dave and R C Joshi, "Secure Data Sharing in Mobile Adhoc Networks," J. International Review on Computers and Software (IRECOS), ISSN 1828-6003 (Peer reviewed and accepted).

[4] A. K. Verma, Mayank Dave and R C Joshi, "Secure Routing in Mobile Networks: A Review," International J. of Systemics, Cybernetics and Informatics (IJSCI), ISSN 0973-4864 (Peer reviewed and accepted).

[5] A. K. Verma, Mayank Dave and R C Joshi, "Applying Distributive Computing In Mobile Ad hoc Networks (MANETs)," peer reviewed and accepted for publication in J. of Punjab Academy of Sciences.

[6] A. Law and W. Kelton, "Simulation Modeling and Analysis," McGraw-Hill, 2000.

[7] A. Menezes, P.Oorschot and S. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996.

[8] A. Perrig, R. Canetti, D. Song and J. D. Tygar, "Efficient and Secure Source Authentication for Multicast," In Proc. of NDSS 2001.

[9] A. Perrig, R. Canetti, J. D. Tygar, and D. Song, "Efficient Authentication and Signing of Multicast

Streams over Lossy Channels," In Proc. of IEEE Symposium on Security and Privacy, 2000.

[10] A. Perrig, Y-C Hu, and D. B. Johnson, "Wormhole Protection in Wireless Ad Hoc Networks," Technical Report TR01-384, Dept. of Computer Science, Rice University.

[11] A. Perrig, R. Canetti, "The TESLA Broadcast Authentication Protocol", Internet Draft, 2000.

[12] Bhupendra Kumar Gupta and B.M.Acharya Manoj Kumar Mishra, "Optimization of Routing Algorithm in Wireless Mesh Networks ", 2009-IEEE.