Journal of Computer Science 4 (5): 353-359, 2008
ISSN 1549-3636

Arithmetic Encoding Based Dynamic Source Routing for Ad-Hoc Networks

Ajay Koul, R.B. Patel and V.K. Bhat
School of Computer Science and Engineering,
Shri Mata Vaishno Devi University, Katra (J&K), India
Department of Computer Science and Engineering,
M. M. Engg. College, Mullana (Ambala), Haryana, India
School of Applied Physics and Mathematics,
Shri Mata Vaishno Devi University, Katra (J&K), India

Abstract: An ad hoc network is a collection of mobile stations forming a temporary network without the aid of any centralized coordinator. Routing messages are an essential component of Mobile Adhoc Networks, as each packet needs to be passed quickly through intermediate nodes from source to destination. Internal threats due to changes in the node behaviour that target the routing discovery or maintenance phase of the routing protocol and security challenges can however lead to insecure communication in MANETS. We proposed a model that found the improper behaviour of the nodes and eliminated them. Also it provided secure routing mechanism of sharing messages between source and destination by modifying and making use of Arithmetic encoding that not only saved the bandwidth but also provided the security by crypting the data. The reason we chose Arithmetic coding was because it typically enabled very high coding efficiency and provided better security.

Key words: Security, dynamic source routing, malicious hosts, ad hoc networks, arithmetic coding

INTRODUCTION

An ad hoc network is a collection of mobile stations forming a temporary network without the aid of any centralized coordinator and is different from cellular network which requires fixed base stations interconnected by a wired backbone. In a mobile ad hoc network (MANET), the nodes act both as traffic sources and as routers that forward packets from other nodes along multi-hop routes to the destination. Such networks are therefore highly insecure as it raises many security issues and threats outside and within the network. Some of the existing protocols[2-5,13] however do provide security but they either safeguard against some attacks due to malicious or selfish node behavior like blackhole, Byzantine etc or provide security against integrity, authentication etc only. To overcome this, a mechanism is required to predict and safeguard against the behaviour of nodes that causes internal threats and also to provide end to end security. In this study we present a simple, secure and bandwidth efficient model for MANET that provides security against attacks by eliminating non cooperative and malicious hosts and by solving security problems like non repudiation, authentication and integrity by encrypting the data. Our method uses a three layered approach wherein first the route is established by Dynamic Source Routing[1], then identification of malicious /selfish nodes takes place and finally end to end security is established using arithmetic coding which not only compresses the data but also provides security by imparting encryption as well.

MOTIVATION

Secure routing especially for mobile ad hoc ``networks (MANETs) is not an easy job especially when the resources are constrained. In order to prevent a packet from malicious attack, there are many protocols in the literature which are implementing the security mechanism for both data and header part of the packets. Below mentioned are some of the surveyed secure ad-hoc routing solutions. The protocols mentioned are mostly reactive in nature. Reactive protocols in general have higher delivery rates than proactive solutions since they transmit routing packets only when data packets need to be sent or when there are topological changes in the network. J Hass and Papadimitriou in[2] proposed

Corresponding Author: Ajay Koul, School of Computer Science and Engineering, Shri Mata Vaishno Devi University, Katra (J and K), India

SRP the secure routing protocol that counters malicious behaviour that targets the topological information but it does not address the protection of data transmission system and also requires security association between each source and destination host. Hu, Perrig and Johnson proposed SEAD Secure efficient Adhoc distance vector[3] which is based on DSDV, it provides robust protection against multiple uncoordinated attacks, but fails against warm hole attacks. SEAD also has higher packet delivery ratio and has more overhead and latency. ARIADNE[4], which relies on symmetric cryptography. It uses a key management system named TESLA (Timed Efficient Stream Loss tolerant Authentication) .However; their system requires synchronized clocks for all the nodes in the network, which we find unrealistic for ad hoc networks. Yi, Naldurg and Kravets[5] proposed ARAN the Authenticated Routing for Adhoc Networks which provides security against authentication and Non Repudiation. However only the major problem lies in the use of Asymmetric key cryptography which is highly costly and it is also not completely immune to wormhole attacks. S.Toner and D'O Mahoney suggested SAR the security aware Adhoc routing as described in[6]. The main idea behind SAR is the utilization of a security metric in place of the standard metrics, such as hop count, for the route discovery and maintenance functions. The security routing metric is defined through attributes that reflect certain security properties, such as authentication, non-repudiation and others. Therefore, the discovered and maintained routes satisfy the requirements of the security metric. However the disadvantages are that security properties in it like time stamp, sequence number, authentication, integrity, etc. have a cost and performance penalty, thus it affects the secure route discovery. So overall many security solutions exist but fail to resolve the security issues and threats simultaneously in Manets. The approach of layered model provided in this study however addresses both the issues of threats and security concerns within and outside the MANETS.

SECURITY PROBLEMS AND ATTACKS

Security is the combination of processes, procedures and systems used to ensure confidentiality, authentication, integrity, availability, access control and non repudiation[7].

Confidentiality is to keep the information sent unreadable to unauthorized users or hosts. MANET uses an open medium, so usually all hosts within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data and another technique is to use directional antennas.

Authentication is to be able to identify a host or a user and to be able to prevent impersonation. In wired networks and infrastructure-based wireless networks, it is possible to implement a central authority at a point such as a router, base station, or access point. But there is no central authority in MANET and it is much more difficult to authenticate an entity.

Integrity is that to be able to keep the message sent from being illegally altered or destroyed in the transmission. When the data is sent through the wireless medium, the data can be modified or deleted by malicious attackers. The malicious attackers can also resend it, which is called a replay attack.

Non-Repudiation is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by it. By producing a signature for the message, the entity cannot later deny the message. In public key cryptography, a host A signs the message using its private key. All other hosts can verify the signed message by using A's public key and A cannot deny that its signature is attached to the message.

Availability is to keep the network service or resources available to legitimate users. It ensures the survivability of the network despite malicious incidents.

Access control is to prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes. In general, access control is the most commonly thought of service in both network communications and individual computer systems. Apart from the above security problems, MANETS also has the problem of attacks on the network. Some of the possible attacks are as follows.

Wormhole attack: An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole [8] [10]. Wormhole attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as DSR or AODV, the attack could prevent the discovery of any routes other than through the wormhole.

Black hole attack: The black hole attack has two properties. First, the host exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination host, even though the route is spurious, with the intention of intercepting packets. Second, the attacker consumes the intercepted

packets without any forwarding. However, the attacker runs the risk that neighboring hosts will monitor and expose the ongoing attacks. There is a more subtle form of these attacks when an attacker selectively forwards packets. An attacker suppresses or modifies packets originating from some hosts, while leaving the data from the other hosts unaffected, which limits the suspicion of its wrongdoing.

Byzantine attack: A compromised intermediate host works alone, or a set of compromised intermediate hosts works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services[9].

Rushing attack: Two colluded attackers use the tunnel procedure to form a wormhole. If a fast transmission path (e.g., a dedicated channel shared by attackers) exists between the two ends of the wormhole, the tunneled packets can propagate faster than those through a normal multi-hop route. This forms the rushing attack. The rushing attack can act as an effective denial-of-service attack against all currently proposed on-demand MANET routing protocols, including protocols that were designed to be secure, such as ARAN and Ariadne[8].

Resource consumption attack: This is also known as the sleep deprivation attack. An attacker or a compromised host can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim host.

Location disclosure attack: An attacker reveals information regarding the location of hosts or the structure of the network. It gathers the host location information, such as a route map and then plans further attack scenarios. Traffic analysis, one of the subtlest security attacks against MANET, is unsolved. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security sensitive scenarios.

SYSTEM MODEL

In the development of the onion model of defense shown in Fig. 1, we have used[11] as base model for providing security in the Ad hoc networks. This model is based on[11]. The First layer of the algorithm is used

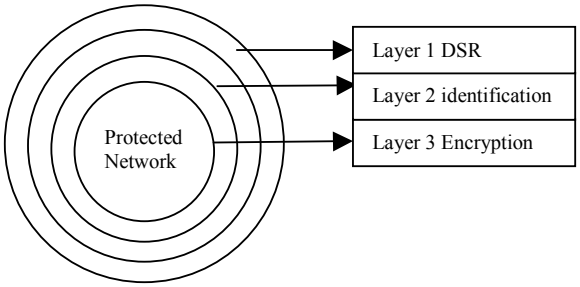

Fig. 2: Onion defense model

to establish the network using DSR as this technique has certain advantages over the other Routing Techniques. The second Layer identifies the Non Co-operative (selfish) as well as the malicious hosts in the network thereby providing security against various attacks (black hole, Byzantine approach, etc.,) as mentioned above. The third and the final layer is used to provide security against Confidentiality, Non repudiation, integrity, authentication, etc. by using an arithmetic encoding approach to compress the data as the bandwidth between the source and the destination is limited so our aim is to transfer maximum data using this limited bandwidth. This technique is further extended to generate random key sequences to crypt the data using a Symmetric key approach mechanism as it is feasible to strengthen the symmetric key method instead of using the public key mechanism because the Public key Encryption and Decryption brings lot of Computational cost for Mobile Devices that do not have much computing power. The distribution of the key is preferably done through the alternate route or through the secured route only if the alternate route does not exist. There are total three keys involved between source and destination. First key is the shared key between CA (certification authority) and the individual hosts. This key is required to provide communication between CA and the individual hosts also required for finding the behavior of the hosts in the network. Second Key is the network shared key which is being issued by the CA at the time of establishment of the network or renewal of the network. This key is used to make sure that hosts possessing the key can only participate in the network. The third type of key is being used between Source and destination. This key is used to crypt the data and offer additional security to it.

Dynamic source routing (DSR): In the developed model we are considering the Dynamic Source Routing (DSR) protocol[12] based security system. Developed model is a simple and efficient routing protocol which is designed specifically for use in multi-hop wireless ad

hoc networks of mobile hosts. The brief of DSR protocol is as follows. It allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. DSR has been implemented by numerous groups and deployed on several test beds. Networks using the DSR protocol have been connected to the Internet. It can interoperate with Mobile IP and hosts using Mobile IP and DSR have seamlessly migrated between Wireless Local Area Networks (WLANs), cellular data services and DSR mobile ad hoc networks.

The protocol is composed of the two main mechanisms of Route Discovery and Route Maintenance, which work together to allow hosts to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead of DSR to scale automatically to only that needed to react to changes in the routes currently in use. The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example for use in load balancing or for increased robustness. Other advantages of the DSR protocol include easily guaranteed loop-free routing, support for use in networks containing unidirectional links, use of only soft state in routing and very rapid recovery when routes in the network change. The DSR protocol is designed mainly for mobile ad hoc networks of up to about two hundred hosts and is designed to work well with even very high rates of mobility.

In DSR a source host that wants to send a packet first checks its route cache. If there is a valid entry for the destination, the host sends the packet using that route; if no valid route is available in the route cache, the source host initiates the route discovery process by sending a special route request (RREQ) packet to all neighboring hosts. The RREQ propagates through the network, collecting the addresses of all hosts visited, until it reaches the destination host or an intermediate host with a valid route to the destination host. This host in turn initiates the route reply process by sending a special route reply (RREP) packet to the originating host announcing the newly discovered route. The destination host can accomplish this using inverse routing or by initiating the route discovery process backwards. The DSR algorithm also includes a route maintenance feature implemented via a hop-to-hop or end-to-end acknowledgment mechanism; the former includes error checking at each hop, while the latter checks for errors only on the sending and receiving sides. When the host encounters a broken link, it sends a route error (RERR) packet. Dynamic source routing is easy to implement, can work with asymmetric links and involves no overhead when there are no changes in the network. The protocol can also easily be improved to support multiple routes to the same destination.

Identification and elimination of malicious/selfish hosts: Developed model provides the first hand protection against active attacks. This model is based on[13] wherein we assume that there exists a Certificate Authority. Any host who wants to participate in the network should get registered with CA. The CA has the many roles to play. Firstly it has to identify the malicious hosts and selfish hosts and informs the other participating hosts about the intensions of these hosts and secondly it has to provide and constantly update the network key common among the participating hosts. Let us say host A wants to Participate in the network. The Host A will approach to CA and provide a shared key and also the MAC Address details to the CA. The CA in turn will send some packets of verification to host A by encrypting the packets with the shared key and physical address and Host A in turn will return the decrypted packets to CA. This way CA will check the validity of the Shared Key between CA and host A and hence will register the host. Now let us say that the Host A is malicious. The CA detects the malicious hosts by sending each host in the network arbitrary route requests one by one. When a CA wants to test whether a host (let's say host A) is forwarding other hosts' data packets inside the network or not, the CA will first pick a destination host that is close to host A. Then, the CA will send a RREQ to host A for the destination host. Once A agrees to participate in the route and a route is established between the CA, host A and the destination host, the CA will send data packets to the destination host using this route. Then, the CA will check whether the destination host has received the packets or not by sending information and asking for the received packets to the destination host encrypted with the shared key of the host. The destination host will send back an acknowledgement to CA whether it has received any data packets from A or not. If it has not, the CA will mark host A as a malicious host and will update the network key immediately. All hosts in the network except for host A will receive the new network shared key. From that point host A will not be able to encrypt or decrypt any packet information. The CA will know that host A is malicious and take it out of the network.

The CA has a list of physical addresses that are allowed to communicate on the network, which are unique to each host in the network. The CA will simply

Table 1: Symbols with probability

Symbol	Probability	Range
a	2	[0.0, 0.5)
b	1	[0.5, 0.75)
c	1	[0.75, 1.0)

Table-2 Coding Table

Symbol	Range	Low value	High value
		0.00000	1.000000
b	1.00000	0.50000	0.750000
a	0.25000	0.50000	0.625000
c	0.12500	0.59375	0.625000
a	0.03125	0.59375	0.609375

take the malicious host's physical address out of the list. This is a technique called physical address filtering. In the developed algorithm, these malicious hosts are left out of the network. The same approach can be applied to filter out selfish hosts. In our approach we treat selfish host's equivalent as malicious hosts as in MANET communication the involvement of selfish and malicious hosts can equally reduce the efficiency of the network drastically.

Modified arithmetic algorithm: The concept of using arithmetic coding has been generated from[14] wherein Binary arithmetic coding with key based interval splitting has been used to obtain compression as well as encryption. The designed algorithm is a simple arithmetic technique but slightly diverted as in this we use position based key number generation which requires less computation and hence suitable for MANETs where power requirement is a constraint[15]. The idea behind arithmetic coding is to have a probability line, 0-1 and assign to every symbol a range in this line based on its probability, the higher the probability, the higher range which assigns to it. Once we have defined the ranges and the probability line, start to encode symbols, every symbol defines where the output floating point number lands. Let us say we have:

Symbols with probability as shown in Table 1. Note that the '[' means that the number is also included, so all the numbers from 0 to 5 belong to a but 5. And then we start to code the symbols (Table 2) and compute our output number. The algorithm to compute the output number is:

- Low = 0
- High = 1
- Loop. For all the symbols
  - Range = high-low
  - High = low + range * high range of the symbol being coded
  - Low = low + range * low range of the symbol being coded

Table3: Range table

Symbol	Probability	Range
A	2	[0.0, 0.5)
B	1	[0.5, 0.75)
C	1	[0.75, 1.0)

Table 4: Decoding table

Symbol	Range	Number
B	0.25	0.59375
A	0.50	0.37500
C	0.25	0.75000
A	0.50	0.00000

Where:

- Range, keeps track of where the next range should be
- High and low, specify the output number
- Randomly select a block of 64 bits and note down its position
- Multiply this output number with a large number preferably of high integer value at the position selected
- Repeat the process for at least half of the total number of blocks (More the random blocks selected more difficult it is to get the data)
- The position and the number for the blocks becomes the key ring which is to be passed to the Destination

For example: The output number will be 0.59375. This number will be multiplied with a number that will serve as the key for source and destination. The Key number will be randomly taken (preferably not less than 5 digit number) and the information of the position where it will be generated and applied will be preserved and passed on to the destination. Let the number be 41885 for the first block. The key generation will be (41885,1) for the first block and for n number of blocks the complete key would be $\{(k_1, p_1), (k_2, p_2), (k_3, p_3), \ldots, (k_n, p_n)\}$ which becomes a key ring where $k_1, k_2, \ldots, k_n$ denotes the key numbers and $p_1, p_2, p_3, \ldots, p_n$ denotes the positions. The output number will be generated from a block of data of 64 bits.

The way of decoding is first to apply key ring to the blocks of data so that the fractional number corresponding to each block is extracted, the number is then first compared in the range table (Table 3) to find the first symbol of the data and then extract the range of this symbol from the floating point number (Table 4). The complete algorithm for extracting the ranges is:

- Loop. For all the symbols
  - Range = high range of the symbol-low range of the symbol

- Number = number-low range of the symbol
- Number = number / range

And this is how decoding is performed.

RESULTS AND DISCUSSION

In this study we have presented a layered approach to provide security to MANETs. This approach when incorporated with any routing protocol can provide better security by identifying and eliminating the malicious/selfish nodes that causes most of the attacks like black hole, wormhole, Byzantine, rushing etc. and also addresses most of the security concerns in MANETS like, confidentiality, integrity, Non Repudiation, Authentication etc. The above approach uses DSR in the first layer however any routing algorithm can be adopted.

Conclusion and future work: The model presented mostly depends on two layers which are responsible for achieving security in MANETS. The Layer two algorithm detects successfully the selfish and malicious hosts thereby providing guard against various attacks. Layer 3 techniques, i.e., the approach of arithmetic encoding used here is the modified form of the algorithm. This algorithm not only compresses data but also provides security by generating the position based keys which is hard to predict thus providing better reliability and security. The purpose of using arithmetic coding is firstly to compress the data so that the bandwidth is utilized less which is a constrain in MANETs and secondly if we apply this technique to a block of 64 bits (8 data bytes) it generates real number values which becomes difficult to interpret if encoded further by a unique different key numbers on different blocks of data. Since the technique mentioned above even though provides a good amount of security but modification in terms of reducing the complexity of the arithmetic encoding algorithm is required as it involves more mathematical calculation and hence may consume more power which is a constrain in Manets

The above mentioned approach uses two important layers to provide security in Manets. The approach even though is theoretical but provides a thorough solution to provide security against nodes with selfish or malicious intent. The layer three approach even though is the older concept used here but the modification in terms of key generation and position based utilization makes it proper for providing additional security.

REFERENCES

1. Johnson, D.B., D.A. Maltz, and J.Broch, "DSR: The Dynamic Source Routing For Multi-Hop Wireless Ad-Hoc Networks," Ad Hoc Net., C.E. Perkins, ed., Addison-Wesley Longman Publishing Co., Inc, Boston,MA,2001,pp: 139-172 ISBN:0-201-30976-9
2. Papadimitratos, P. and Z.J. Haas, 2002. Secure routing for mobile ad hoc networks. In: SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, (CNDS 2002), San Antinio, Texas, Jan 2002,pp. 27-31,
3. Hu, Y.C., D.B. Johnson and A. Perrig, 2003. Secure efficient distance vector routing for Mobile wireless Adhoc networks. Adhoc Networks J., 1: 175-192.
4. Hu, Y.C., A. Perrig and D.B. Johnson, 2002. Ariadne: A secure on-demand routing protocol for ad hoc networks. In: Proceeding 8th ACM International Conference Mobile Computing and Networking (Mobicom'02), Sept. 2002, Atlanta, Georgia, pp: 12-23.
5. Yi, S., P. Naldurg and R. Kravets, 2001. Security-aware ad hoc routing for wireless networks. In: Proceedings of the 2nd ACM Symposium Mobile Ad Hoc Networking and Computing (Mobihoc'01), Oct. 2001, Long Beach, CA, pp: 299-302.
6. Toner, S. and D. O'Mahony, 2003. Self-organizing node address management in ad hoc networks. Pers. Wireless Commun., IFIP-TC6 8th Int'l. Conf. (PWC 2003), Sept 23-25, Venice, Italy,2003, pp. 476-83.
7. Ning, P. and K. Sun, "How to misuse, AODV: A case study of inside attacks against mobile ad-hoc routing protocols". In: Proceedings of the IEEE Workshop on Information Assurance, United States Military Academy, West Point, NY.18-20 June,2003 pp. 60-67 ISBN 0-7803-7808-3/03
8. Ilyas, M., 2003. The Handbook of Ad Hoc Wireless Networks. CRC Press, USA, ISBN:0-8493-1332-5 pp: 5-6.
9. Awerbuch, B., D. Holmer, C. Nita-Rotaru and H. Rubens, "An on-demand secure routing protocol resilient to byzantine failures". In: Proceedings of the ACM Workshop on Wireless Security, Atlanta, Georgia, Sept 2002, pp: 21-30.

10. Sanzgiri, K., B. Dahill, B. Levine, C. Shields and E. Belding-Royer, " A secure routing protocol for ad hoc networks", In: Proceedings of IEEE International Conference on Network Protocols (ICNP'02), Nov. 12-15,IEEE Press, Paris, 002, pp: 78-87.
11. Hu, Y., A. Perrig and D. Johnson, 2002. Ariadne, A secure on-demand routing for ad hoc networks. In: Proceedings of 8th ACM Int'l. Conf. Mobile Comp. and Net.(Mobicom'02), Atlanta, Georgia, Sept. 23-28, 2002, pp.12-23.
12. Johnson, D.B., D.A. Maltz and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks" in Ad Hoc Networking. In: Perkins, C.E. (Ed.). Addison-Wesley, Longman Publishing Co., Inc, Boston,MA,2001,pp: 139-172. ISBN:0-201-30976-9
13. Weeks, M. and G. Altun, 2006. Efficient secure dynamic source routing for ad-hoc networks. J. Networks Syst. Manage., Vol 14, No. 4, Dec 2006, pp. 559-581 DOI: 10.1007 /s 10922-006-9043-8
14. Wen, J., H. Kim and J.D. Villasenor, 2006. Binary arithmetic coding with key based interval splitting. IEEE Signal Proc. Lett., 13. , Issue 2, pp. 69-72, DOI 10.1109/LSP.2005.861589.
15. Langdon, G. and J. Rissanen, 1981. Compression of black-white images with arithmetic coding. IEEE Trans. Commun., COM-29: 858-867.