International Journal of Engineering Research & Management Technology ISSN: 2348-4039

March- 2015 Volume 2, Issue-2

Email: editor@ijermt.org www.ijermt.org

Improved Routing Security in Wireless Mobile ADHOC Network

Mr.Anand Pandey
Assistant Professor
Department of IT
SRM University NCR Campus
Modinagar

Sakshi Khurana, Ayush P.Kumar
B.Tech Student
Department of IT
SRM University NCR Campus
Modinagar

ABSTRACT
Ad hoc techniques play a major role in security and intelligence companies. Mobile Ad-hoc networks are collection of wireless mobile devices with limited broadcast range and resources, with no fixed infrastructure. A routing security issue is one of the most important issues in ad-hoc networks. At the physical level, wireless channels offer poor protection to protocol packets and are susceptible to signal interference, jamming, eavesdropping, and distortion.
We will discuss some flaws in earlier protocols (e.g. Ariadne) and proposes solutions to overcome them by adding the technique of malicious node detection. It also focuses on reducing overhead of route discovery and maintenance.

Keywords: Ad hoc network, MAC (Message Authentication Code), MANET, Ariadne

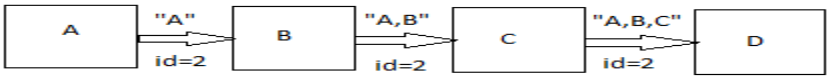
INTORDUCTION

Ad hoc techniques play a major part in these networks and thus grow in popularity. Ad hoc means "Arranged or happening when necessary but not planned in advanced". Wireless networks are everywhere nowadays, whether deployed as sensor networks for seismic activities in earthquake endangered areas, weather stations. With the amount of actually used wireless ad-hoc networks, the question about new and secure routing techniques arises. Old methods and algorithms fail to acquire acceptable performance since they were not designed for wireless use. While many of the new proposed routing protocols i.e. Ariadne it is easy to configure that the attack has taken place. Moreover, the detection of the malicious node is there. Among the proposals for this kind of combination, there is one which is named Ariadne It uses highly efficient symmetric authentication mechanisms to reduce computing time, detection of malicious node and proactive route maintenance.

LITERATURE SURVEY

DSR

D. Johnson et al(1999) [1] on **"The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad-Hoc Networks".** DSR is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes.Two mechanisms of Route Discovery and Route Maintenance like Packet Salvaging, Automatic Route Shortening, Caching Negative Information used in DSR.G. Reddy et al(2012) [2] **"Enhancing DSR Protocol Performance in Mobile Ad-hoc Network using Proactive Route**



Maintenance (PRM**)".**

The above figure shows how there is specific constant id is used that is "2" in this.The node list increases with each node from A to ABC.If A want to send request to D then it passes through each intermediate node as RREQ and route reply as RREP.

ARIADNE

B. May et al (2009) [3]"**Ariadne: Secure On-Demand Routing in Ad-Hoc Networks**". Ariadne is a secure on-demand ad-hoc routing protocol.DSR is used as the routing groundwork for Ariadne. It is about secure authentication of routing information only, not about privacy or encryption.

Assumptions

Ariadne only works on bidirectional link.It proposes a number of attacker scenarios and attack types Attackers can be divided into two classes: **passive** (the eavesdropping kind) and **active** (the manipulating kind). Ariadne does in fact address all the issues of DSR such as:Black holes are nodes dropping incoming packets ,Gray hole ,Vertex cut or forging routing information ,blackmailing nodes, this is done by maligning good nodes, causing them to be blacklisted.

TESLA

R. Canetti et al (2002)[4]"The TESLA Broadcast Authentication Protocol" TESLA (Timed Efficient Stream Loss-tolerant Authentication).TESLA is a broadcast authentication protocol which includes low computation overhead for generation and verification of authentication information, low communication overhead, limited buffering required for the sender and the receiver and timely authentication for each individual packet.

ASSUMPTIONS

One Way Chain, loose time synchronization, overhead increment is there. Due to its usage there is increase in the complexity level that is adjourned in the further discussion.

EXISTING PROBLEMS

The earlier used methods of the ariadne and DSR uses basically the MAC and the Hash function.In the MAC function it sums the numeric values of its arguments (converted from hexadecimal to decimal notation) and then pads the last 3 digits of the result between values P and Q to give the resultant string as = P"((dec(a)+dec(b)+dec(c)+….))"Q. This has been done to maintain MACs as 5 characters in length and easier to compute for practical purpose in our example. In further computation process which uses the , we use a very simple hash function for generating one way key chains. Using the function H["p","abcd"] it removes the leftmost bit from the string and shifts the string one character to the left, and concatenates the argument as rightmost bit to give the result: "bcdp".

Route Request has parameters ROUTE REQUEST (initiator, target, id, time interval, hash chain, node list, MAC list)

Id is a random value, say 125. Time interval is 5 units.

MAC is MAC (initiator, target, id, time interval,hash chain,Node list,Key (initiator,target))

ALGORITHM

1. S : h0 = MACKSD (RREQ, S, D, id, ti)
2. S− > ¤ :< RREQ, S, D, id, t i, h0, (), () >
3. A : h1 = H[A, h0]

MA = MACKAti

(RREQ, S, D, id, t i, h1, (A), ())

4. A− > ¤ :< RREQ, S, D, id, ti, h1, (A), (MA) >

PROPOSED SOLUTION

Based on this previous algorithm we found the way to the new algorithm. The previous one did not have any method for detecting exactly which node was malicious. This feature was introduced in the new algorithm.

MODIFIED ROUTE REPLY As the new security methods applied were in Route Reply stage, the Route Request stage was left as it is. The proposed solution is to use 2 single MACs along with MAC list for detecting attacker node; by keeping track of nodes that are two hops away. Considering backward security, the modified Route Reply would have parameters:

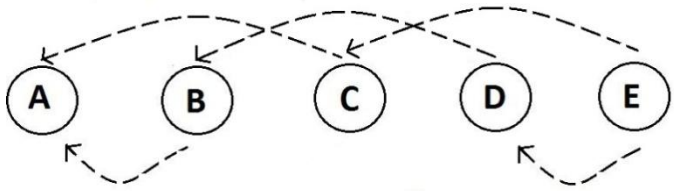
ROUTE REPLY (target, initiator, time interval, node list, MAC list, $SMAC_1$, $SMAC_2$, target MAC, key list).

For a path A-B-C-D-E; consider node d:

Route reply from C to B,

$SMAC_1$ is calculated as MAC(target, initiator, time interval, node list, target MAC, Key(D,B)). $SMAC_2$ is calculated as MAC(target, initiator, time interval, node list, target MAC, Key(C,A)).

That is, key values of nodes two hops away are used (except at the end nodes for which key value of node one hop away is used) as stated in diagram:



Two Hop Backward Checking

Pro-Active Route Maintenance Algorithm

Pro-active route maintenance is used for reducing the overhead and hence enhancing the communication. Pro-active route maintenance has a simple algorithm which instead of creating a single backup path, has multiple paths.

REFERENCES

1. M. Bellare, R. Canetti and H. Krawczyk, Keying hash functions for message authentication, in: Advances in Cryptology – Crypto'96, Lecture Notes in Computer Science, Vol. 1109, pp. 1–15, 1996.
2. .Broch, D.A.Maltz, D.B. Johnson, Y.C.Hu and J.G. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols", Proceedings of the 4th ACM/IEEE International Conference on Mobile Computing and Networking, pp. 17-26, 1998.
3. David B. Johnson, David A. Maltz, Josh Broch, "DSR: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Computer Science Department Carnegie Mellon University Pittsburgh, pp. 1-22, 1999.
4. D.A. Maltz, J. Broch, J. Jetcheva and D.B. Johnson, "The effects of on-demand behavior in routing protocols for multi-hop wireless ad hoc networks", IEEE Journal on Selected Areas in Communications 17(8), pp. 1439–1453, 1999.
5. Adrian Perrig, Ran Canetti, J.D. Tygar, Dawn Song, "The TESLA Broadcast Authentication Protocol", pp. 1-16, 2002.
6. D. Coppersmith and M. Jakobsson, Almost optimal hash sequence traversal, in: Proceedings of the 4th Conference on Financial Cryptography (FC'02), Lecture Notes in Computer Science, pp. 102–119, 2002.