International Journal of Innovation Education and Research

ONLINE ISSN: 2411-2933 PRINT - ISSN: 2411-3123

Mitigating Routing Attacks in Mobile Ad Hoc Networks

Dr. Ahmed Khameis Sharf Eldin Elkabour;Dr. Rahma Teirab Abaker Haroun

Abstract

Mobile Ad hoc Networks have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. In existing solutions typically attempt to isolate malicious nodes based on binary or naive fuzzy response decisions. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure. In this paper proposes a risk-aware response mechanism to systematically cope with the identified routing attacks. To avoid the routing attacks Dijkstra's and Destination sequenced Distance Vector algorithm are used. Dijkstra's algorithm solves the single-source shortest-path problem when all edges have non-negative weights. The primary improvement for ad hoc networks made in DSDV over conventional distance vector is the addition of a sequence number in each routing table entry.

Keyword: Intrusion response, risk aware, dempster- shafer theory, Dijkstra's algorithm, Destination sequenced Distance Vector.

Published Date: 7/31/2019 **Page.227-233** **Vol 7 No 7 2019**

DOI: https://doi.org/10.31686/ijier.Vol7.Iss7.1603

Mitigating Routing Attacks in Mobile Ad Hoc Networks

Dr. Ahmed Khameis Sharf Eldin Elkabour
Department of ET, Nyala Technical College, Sudan Technical University, Sudan
'E-mail. kabour2006@hotmail.com

Dr. Rahma Teirab Abaker Haroun
Computer Science & IT Dept., Nyala Technical College, Sudan Technical University, Sudan
Dept. of Math, University College in Alkhafji, University of Hafr Al Batin, Saudi Arabia
E-mail. toha124@gmail.com
Contact number. 00966543219226

Abstract

Mobile Ad hoc Networks have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. In existing solutions typically attempt to isolate malicious nodes based on binary or naive fuzzy response decisions. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure. In this paper proposes a risk-aware response mechanism to systematically cope with the identified routing attacks. To avoid the routing attacks Dijkstra's and Destination sequenced Distance Vector algorithm are used. Dijkstra's algorithm solves the single-source shortest-path problem when all edges have non-negative weights. The primary improvement for ad hoc networks made in DSDV over conventional distance vector is the addition of a sequence number in each routing table entry.

Index Terms **-** Intrusion response, risk aware, dempster- shafer theory, Dijkstra's algorithm, Destination sequenced Distance Vector.

I INTRODUCTION

Mobile Ad-hoc Network (MANET) is a mobile network which has a large scale of self-directed nodes which is powerful to form a short-term means of communication network, without any use of prior communications.

MANET contains dynamic topology, does not rely on the static communications and neither it contains any kind of base control station into the networks hence this made a challenging area of research in networks. It has a limited amount of range of the communication and capabilities of power consumptions hence in real time scenario, it can be used in the military during the battle fields, during the disastrous earthquake and recovery from those disaster. [1].

The performance of ad hoc networks depends on cooperation and trust among distributed nodes. To enhance security in ad hoc networks, it is important to evaluate trustworthiness of other nodes without centralized authorities. Security is an essential requirement in mobile ad hoc network [2].

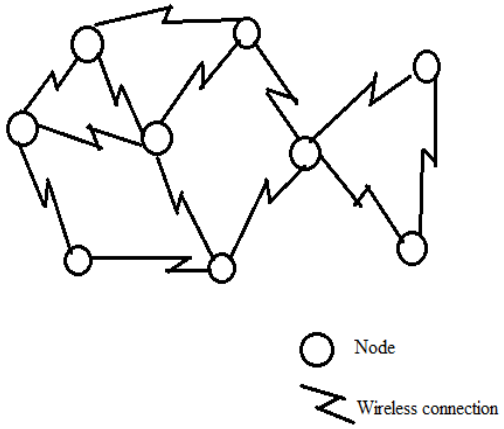

Fig. 1. Mobile Ad hoc Networks

In D-S theory has been adopted as a valuable tool for evaluating reliability and security in information systems and by other engineering fields. D-S theory support Dempster's Rule of Combination (DRC) it is associative and no weighted. In MANET, improper countermeasures may cause the unexpected network partition, bringing additional damages to the network infrastructure. Binary response method is only count the attacks. To address these limitations in MANET intrusion response scenario, we introduce a new Dempster's rule of combination with a notion of importance factors (IF) in D-S evidence model [1] [3].

The blackhole attack has two properties. First, the node exploits the mobile ad hoc routing protocol, such as AODV, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets [8]. Second, the attacker consumes the intercepted packets without any forwarding. However, the attacker runs the risk that neighboring nodes will monitor and expose the ongoing attacks referred as fig 2.

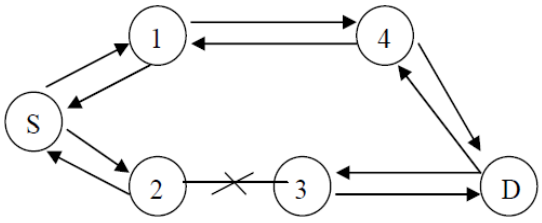

Fig. 2. Black hole attack

II RELATED WORKS

Mojtaba GhanaatPisheh Sanaei et. al. [5] proposed investigated the current routing attacks and countermeasures in a MANET. Our studies showed how the attacks can compromise the routing protocols, Some solutions that rely on cryptography and key management seem promising, but they are too expensive for resource-constrained MANETs.

Although some solutions work well in the presence of one malicious node, they might not be applicable in the presence of multiple colluding attackers.
Some solutions may require special hardware such as a GPS or a modification to the existing protocol.

Sagar R Deshmukh et. al. [7] proposed, An AODV-based secure routing mechanism used to detect and eliminate black hole attack and affected routes in the early phase of route discovery. A validity value is attached with RREP which ensures that there is no attack along the path. The proposed method is simulated in NS2 and performance analysis is carried out.
This system neither requires heavy processing nor extra memory. With the addition of negligible overhead, black hole attack is prevented before actual data transmission phase, even before the participation of malevolent node in the network. Hence the legitimacy of route is confirmed. Proposed strategy is compatible with other reactive routing protocols.
The method will be implemented for other reactive routing protocol as a part of future work.

Viswa Jhananie K.R. [4] proposed The Methodology we use two solutions to prevent nodes from black hole attack. They are An efficient algorithm using watchdog :
Here given two different solutions(i) algorithm using watchdog and (ii) two way routing protocol for blackhole attack, in our simulation, we have used random way point model for watchdog and city section mobility model for two way routing protocol. The simulation results shows better performance in throughput under two way routing protocol. The number of packets delivered is more when watchdog is used and the delay is also consistently reduced under watchdog method. So, we conclude that watchdog can be considered as a better solution in securing data from blackhole attack.
For future enhancement we have used random waypoint model and city section mobility model for our simulation. The same work can be carried over with different mobility models and with different protocols. [4].

S. S. Jadhav et. al. [9] proposed, Performed simulation and measured DSR algorithm for normal condition and same parameters are measured after applying disaster condition on nodes and the simulation results of disaster prevention condition are mentioned.
It is observed that the performance of the network after application of prevention condition is nearly same as the normal performance. The performance is evaluated in terms of Network Throughput, Packet Delivery Ratio, and Average end to end delay . [9].

III RISK AWARE RESPONSE MECHANISM

An adaptive risk aware response mechanism based on quantitative risk estimation and risk tolerance [1]. Risk aware response mechanism is divided into the following four steps referred as in fig. 3.
Evidence collection

In evidence collection Intrusion Detection System (IDS) gives an attack alert with a confidence value and it forms a vital component of internet security. Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack.
Risk assessment

Risk assessment consists of an objective evaluation of risk in which assumptions and uncertainties are clearly considered and presented. Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory.

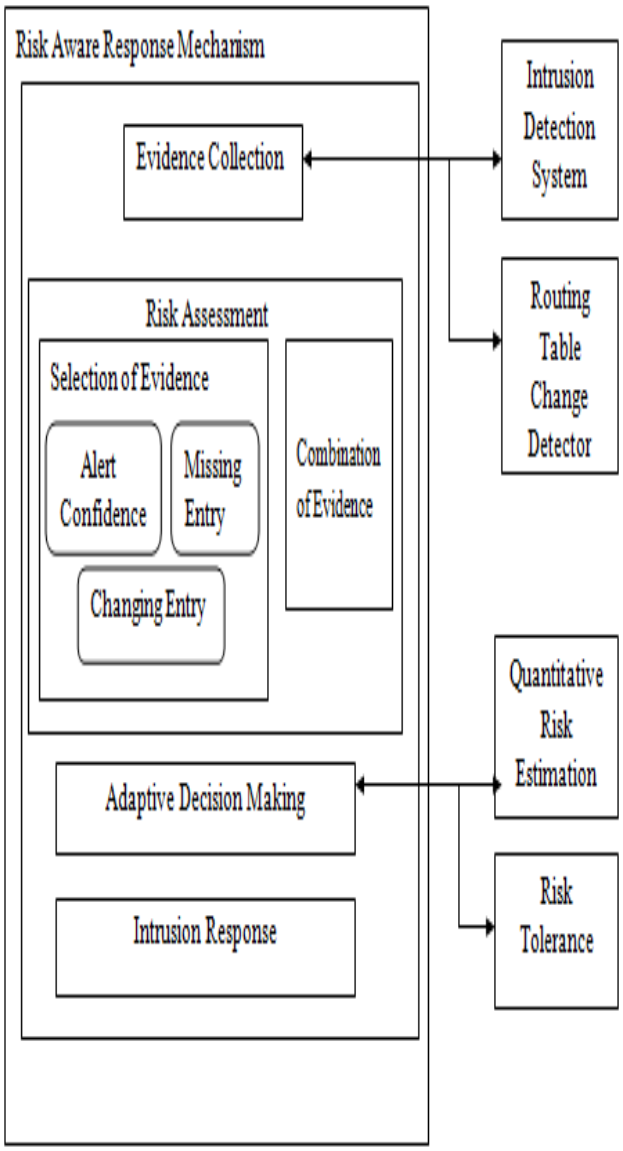

Fig. 3. Risk aware response mechanism

Risk of countermeasures is calculated as well during a risk assessment phase.

Decision making

The adaptive decision module provides a flexible response decision-making mechanism, which takes risk estimation and risk tolerance into account. To adjust temporary isolation level, a user can set different thresholds to fulfill her goal.

Intrusion Response

With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner.

IV DIJKSTRA'S ALGORITHM

Dijkstra's algorithm solves the single-source shortest-path problem when all edges have non-negative weights. Algorithm starts at the source vertex, s, it grows a tree, T, that ultimately spans all vertices reachable from S. Vertices are added to T in order of distance i.e., first S, then the vertex closest to S, then the next closest, and so on. EXTRACT_MIN takes O(V) time and there are |V| such operations. Therefore, a total time for EXTRACT_MIN in while-loop is $O(V^2)$. Since the total number of edges in all the adjacency list is |E|. Therefore for-loop iterates |E| times with each iteration taking O(1) time.

Hence, the running time of the algorithm with array implementation is $O(V^2 + E) = O(V^2)$ .If G is sparse, EXTRACT_MIN operations takes O(lg V) time and there are |V| such operations. The binary heap can be build in O(V) time. Operation DECREASE (in the RELAX) takes O(lg V) time and there are at most such operations. Hence, the running time of the algorithm with binary heap provided given graph is sparse is O ((V + E) lg V).

```
1 Initialization (u = source node):
2 N' = {u} /* path to self is all we know */
3 for all nodes v
4 if v adjacent to u
5 then D(v) = c(u,v) /* assign link cost to neighbours */
6 else D(v) = ∞
7 Loop
8 find w not in N' such that D (w) is a minimum
9 add w to N'
10 update D(v) for all v adjacent to w and not in N' :
11 D(v) = min( D(v), D(w) + c(w,v) )
12 /* new cost to v is either old cost to v or known
13 shortest path cost to w plus cost from w to v */
14 until all nodes in N'
```

V DESTINATION SEQUENCED DISTANCE VECTOR

In DSDV the existence of stale route does not imply that there is no valid route to the destination. The packets can be forwarded thru other neighbors who may have routes to the destination. When an immediate link from the host say 'S' to the destination say 'T' breaks, the proposed protocol creates a temporary link thru a neighbor which has a valid route to the desired destination. The temporary link is created by sending one-hop ROUTE-REQUEST and ROUTE-ACK messages [6].

The host say ‘S’ upon finding the next hop broken link broadcasts a one-hop ROUTE-REQUEST packet to all its neighbors. In turn, the neighbors returns the ROUTE-ACK if it has a valid route to the destination and the host ‘S’ is not the next hop on the route from the neighbor to the destination. Each entry in the routing table has an additional entry for route update time. This update time is embedded in the ROUTE-ACK packet and is used in selecting a temporary route. In case of receiving multiple ROUTE-ACK with the same number of minimum hops , ad hoc host ‘S’ chooses that route which has the latest update time. Therefore, it may be surmised that the proposed Eff-DSDV follows the conventional DSDV but reduces the packet loss due to broken links [6].

Algorithm:

```
Eff-DSDV (Host A, Destination D,
  MAXBufferSize N, Packet X)
1. if (A. NextHopLink () == ACTIVE) then
            Use Standard DSDV;
       else if (A. BufferLength () == N) then
            Discard X;
       else
             place X in A.Buffer;
2. A. Broadcasts (ROUTE-REQUEST, 1, D, A);
3. if (A. NEXT_NEIGHBOR has route to ‘D’) then
            A. RECIEVE (ROUTE_ACK)
4. Min_Hops = ∞; Next_Hop =0;Updated_Time=0;
5. While (Host A has ROUTE_ACK Packets)
   {
    if ( ROUTE_ACK.HOP_COUNT< =Min_Hops )
       {
        if ( ROUTE_ACK.HOP_COUNT =Min_Hops )
       {
        if ( ROUTE_ACK.UPDTD_TIME >                                    Updated_Time )
          {
           Host_ID = ROUTE_ACK.HOST_ID;
           Updated_Time =          ROUTE_ACK.UPDTTD_TIME;
           }
          }
          Else
          {
          Min_Hops = ROUTE-ACK.HOP_COUNT;
          Host_ID = ROUTE_ACK.HOST_ID;
          Updated_Time    ROUTE_ACK.UPDTTD_TIME;
```

```
        }
      }
    }
```

6. Forward the incoming Packet ‘X’, via Host_ID;

VI CONCLUSION

We conclude that The binary response techniques typically attempt to isolate malicious nodes based on binary or naive fuzzy response decisions. However, binary responses may result in the unexpected network partition, causing additional damages to the network infrastructure, and naive fuzzy responses could lead to uncertainty in countering routing attacks in MANET. Therefore to solve all those issues like routing attacks and unexpected network partition in the network with some modifications and methodologies.To overcome these problems Risk aware mechanism, Dijsktra’s Algorithm and DSDV is used. Risk-aware response solution to systematically cope with the identified routing attacks. Especially, this approach considered the potential damages of attacks and countermeasures. In order to measure the risk of both attacks and countermeasures.

REFERENCES

[1] Uzma Shaikh , Arokia Paul Rajan , Intrusion detection and avoidance of black and grey hole attacks using AODV protocol based MANET , International Journal of Engineering & Technology, 7 (1.2) (2018) 110-116 .

[2] Y. Sun, W. Yu, Z. Han, and K. Liu, “Information Theoretic Framework of Trust Modelling and Evaluation for Ad Hoc Networks,” *IEEE J. Selected Areas in Comm., vol. 24, no. 2,* pp. 305-317, Feb. 2006.

[3] Hui Wang and Sally McClean, “Deriving Evidence Theoretical Functions in Multivariate Data Spaces : A Systematic Approach,” *IEEE Transactions on Systems, vol. 38, No. 2, APRIL 2008.*

[4] Viswa Jhananie K.R , An Efficient Algorithm for Detecting and Removing Black hole Attack for Secure Routing in Mobile Ad-hoc Network , International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 5 (2016) .

[5] Mojtaba GhanaatPisheh Sanaei , Imran Ghani , Aida Hakemi , Seung Ryul Jeong , Routing Attacks in Mobile ad hoc Networks : an overview , 123Faculty of Computing, Universiti Teknologi Malaysia (UTM), Johor Bahru 81300, Malaysia 45School of Business Information Technology, Kookmin University, Korea . Sci.Int.(Lahore),25(4),1031-1034,2013 ISSN 1013-5316; CODEN: SINTE 8 1031

[6] Khaleel Ur Rahman, A Venu Gopal Reddy and Rafi U Zamen, “An Efficient Destination Sequenced Distance Vector Routing Protocol for Mobile Ad Hoc Networks,” *International Conference on Computer Science 2008.*

[7] Sagar R Deshmukh , P N Chatur , Nikhil B Bhople , AODV-Based Secure Routing Against Blackhole Attack in MANET, IEEE International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India .

[8] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, “ A Survey of Routing Attacks in Mobile Ad Hoc Networks,”*IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85- 91,Oct 2007.*

[9] S. S. Jadhav, A. V. Kulkarni , R. Menon, "Mobile Ad-Hoc Network (MANET) for disaster management," 2014 Eleventh International Conference on Wireless and Optical Communications Networks (WOCN), Vijayawada, 2014, pp. 1-5.