ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 10, October 2016

Detection of Malicious Packet Dropping Attacks in Wireless Ad Hoc Networks Using Enhanced HLA Scheme

[1] Kasa Hima Bindu [2] S.Vasundra
[1]M. Tech, Dept. of CSE, JNTUA, AP, India
[2] Professor & HOD, Dept. of CSE, JNTUA, AP, India

Abstract: **-- In ad hoc networks and multi-hop wireless networks, packet dropping because of malicious nodes is the major cause of packet loss. To determine whether the losses are caused at the intermediate nodes or at the source and destination itself, a scheme has to be adopted where every node should be checked properly. By using packet loss patterns and with the help of proposed algorithm, the packet dropping nodes can be truthfully detected in a wireless ad hoc environment. The existing system adopted an algorithm which finds packet drops made by insider that are important to the network. Even though the packet drops may be caused by malicious dropping as well as by normal channel losses, the phenomenon which is exhibited has two different correlation structures. The correlations in between the lost packets positions are calculated to find out the detection accuracy. A homomorphism linear authenticator based public auditing architecture allows the auditor to check the correctness of the information given by the packets. A packet block based algorithm is also adopted to achieve the detection accuracy for the sensors with lower computational complexities. Though the system is collusion proof and gives overheads that are large, it is limited to static wireless ad hoc networks. The drawback is that the existing system assumed that source and destination are not malicious in following the protocol. The proposed system modifies the algorithms used in the existing system and detects the malicious routing attacks in ad hoc network. High detection accuracy is achieved by using enhanced HLA scheme where signatures are generated for each node in the route. The advantage of the proposed system is that even the misbehaving source and destination will also be considered in the new system.**

Index terms: **-- Source, HLA scheme, Authentication, Security**

I. INTRODUCTION

Nodes operate in receive and pass on method in a multi hop wireless environment. The opponent may exploit the knowledge of the route and may try to drop the packets and may launch intruder attacks [2][5]. For example, the intruder may behave as helping node in finding process of the route. After getting joined in the route, the intruder may start to drop the packets and in worst scenario the adversary may simply stop forwarding the packets, completely destroying the path between source and destination [12]. This may result in the splitting up the topology. Though packet drops degrades the performance, these kind of packet droppings are easy to find out and repair. Since, there is always an attack at the particular node, it is easy to find out that particular node and delete the node from the topology. If suppose the attack has been detected but the adversary is not detected, Randomized multi path routing algorithm can be used. In this method, it creates three copies and sends the copies of the packets along three paths where two packets are randomly selected. The next node will accept the node in which at least two packets are same [3][2]. A malicious node present in the route can behave friendly during the route discovery and in the later stages may try to drop the packets which are highly important to the network. In most of the cases, dropping packets in small numbers which are important to the network will highly degrade the network performance. This kind of attacks is intermittent and highly difficult to find out.

Finding these kind of selective drops are highly challenging in a dynamic topology [4][6]. Since, both the place and also whether the drop is intentional or not. The drops can be due to two reasons. One is malicious attack and the other kind of drops can be due to the harsh channel conditions. In a wireless dynamic environment, the links keep on breaking and hence maintaining the proper link is the main criteria than detecting the malicious attacks [1][3][8]. Since the link errors are also quite common and cannot be neglected in a wireless topology, it becomes very easy for the intruder to hide under the background of harsh channel conditions. In such a case, just by observing the number of packet losses caused, it is impossible to say whether the losses are due to an intruder or due to the link errors.

On the other hand, even if it is possible to find the differences between the errors caused because of link and malicious errors, the detection algorithm has to be highly precise and requires the malicious drops to be more than link drops to get moderate detection accuracy. It works only when the source and the destination nodes are truthful [4][12]. In this paper, the random nature of source and destination are taken into account. It also checks whether the source and destination are truthful or not. .

II. RELATED WORK

The total work in the related work has been divided into two parts. The first part focuses on the nodes which are almost malicious. It assumes that almost all the packets drops are due to the intruder only which is practically not correct. The link errors are totally ignored in this category. These four categories are further divided into four sub divisions. The first is the credit system. The node which successfully passes on the packet receives a credit [6][10]. The node with least credit is deleted from the route. The second is the reputation system. In this the neighbor has to monitor the next nodes. If a neighboring nodes continuously keep on dropping the nodes. It eventually gets bad reputation and can be avoid from the route. The third is the acknowledgements. The one which is not properly sending acknowledgements can be deleted from the route. The fourth category uses cryptographic techniques.

The second category aims at the situation where the malicious dropping of packets as well as the link errors lead to the packet dropping [9][11]. The traffic rate at source node is compared with the estimated receive rate and then, the reason for the packet dropping effect is decided with detection algorithm. All the above specified methods work well only when the malicious attacks are greater than the link errors.

The present work focuses on the situation where the link errors as well as malicious packet dropping lead to comparable packet loss rates [12][6]. It also takes into source and destination as normal nodes and verifies the identity of the nodes.

III. PROPOSED WORK

Consider some arbitrary path between source and destination. Let it be PSD. The source keeps on sending the packets to destination D through intermediate nodes i1, i2, i3,…,ik , where in+1 is the downstream node of in , for 1≤n≤k-1. The source is aware of the path between source and destination. By performing a trace route operation the source can recognize the nodes in the path PSD. Each hop along the path PSD alternates between the good and bad states. The successful packets are those that are transmitted through the good state and that are transmitted through bad states are lost ones. Since the channel is not dynamic, the autocorrelation function $f_c(x)$, where x is the time lag in the packets is almost static and do not change with time.

3.1 Calculation of fc(x)

Consider m packets are being sent over the channel. The receiver gets the realization of channel state (b1,…,bm),by noticing whether the packet are transmitted or dropped, where bj € {0,1} for j=1,…,m. 1 denotes packet that is successfully received at a node and 0 denotes packet which is dropped at a node. $f_c(x)$ is derived from the autocorrelation function of the sequence :

$f_c(x)$=defE{bj,bj+i} for i=0,…,m.

The expectation value is calculated for all the packets that are transmitted. The correlation between the successful or lost packets at various times is given by the auto correlation function.

3.2 Malicious Activity Model

The malicious node resides secretly in the path and causes degradation in the network performance by dropping the packets. The malicious node can drop any selective number of packets which are very important to the performance of a network or it can drop packets at regular or random intervals. There can be any number of malicious packets between the source and destination along the path PSD. There can also be a backward channel that exists between any two malicious nodes. Therefore the malicious nodes can remain undetected along the path. Even the auditor believes that the packets received successfully because of this covet communication

3.3 Routing Algorithm

The routing employed is based on the nearest neighbours [3][4][1]. Each node keeps the list of the nodes which are nearer to it by certain distance d. The routing is then carried out by taking the least distance node till the destination is reached.

```
❖ Set m nodes
❖ For (i=0;i<m;i++) for 'm' nodes
      ❖ Set i(x,y) coordinates
❖ For (j=0;j<m;j++) repeated m times
      ❖ If(j!=i)
      ❖ Set j(x,y) coordinates
      ❖ (x,y)=i(x,y)-j(x,y)
❖ Evaluate distance d=sqrt(x*x+y*y)
      ❖ D=distance(I,j)
❖ If d<D
      ❖ Append neighbourlist(i)
      ❖ Sort neighbourlist(i)
❖ Enter source_id and destination_id
      ❖ T_id=s_id
      ❖ While(t_id!=d_id)
❖ Route first node in t_idneighbour list
❖ Update t_id with neighbour
❖ Repeat till t_id reaches destination
```

3.4 Enhanced HLA Scheme

In enhanced HLA scheme, a packet loss bitmap is collected from every node in order to calculate the correlation between the lost packets patterns correctly [9][7]. In this, enhanced HLA method is used to solve the purpose. In this scheme the auditor will have the HLA secret key and it generates ∑HLA signatures h1,…,hm. The source tells the auditor how many messages are there for transmission. Then, the auditor sends those many HLA signatures for every individual message [7][6][9]. At any point, The individual keys are created so that it can build a valid HLA key for any random messages combination of, m1,…,mn. $\sum_{i=1}^{m} ci\, ri$, even when not knowing the original HLA secret key. Any intermediate node can generate a valid HLA signature even without knowing the HLA secret key only when all the messages are properly received without being dropped. When the auditor asks a node to submit individual HLA keys only a node which has properly received all the messages with proper HLA keys only can report all the keys. The one which cannot submit keys is checked for its malicious activity.

In the present system, the correlation between the positions of lost packets are considered. This is more efficient than the conventional methods which consider only the number of lost packets. Even if either the source or destination is false, the system fails. For example in conventional system, the detection of malicious activity is modelled as binary hypothesis test, in which B_0 is the consideration that no malicious node is present which means , if there are any packet drops, they are completely because of link errors. B_1 is the consideration that there is some malicious activity in the link with combined effect of errors due to link failures and malicious dropping. After some time period t, let the number of lost packets that are observed in the link be M.

M=a under B_0(absence of malicious activity)

M=a+b under B_1(presence of malicious activity)

Where 'a' and 'b' are the packet drops caused due to link and malicious droppings, respectively. 'a' and 'b' are random variables. Let h_0(M) and h_1(M) be the probability density functions on B_0 and B_1 respectively. Let Pf and Pm be the false alarm and detection due to miss accuracy probabilities. The total detection error is given by

Pdedef=0.5(Pf+Pm)

If M<Mth , accept B_0,
Otherwise, accept B_1,

Where Mth is the solved value of the equation h_0(Mth)=h_1(Mth).This approach fails when the packet drops are highly selective. Mere counting of packet drops alone cannot determine the malicious activity when the packet drops become highly selective an this incur adversely affects the network performance.

3.5 Malicious Activity Detection

When a malicious activity is sensed by destination, then it immediately informs the auditor DA [8][12]. Then the public auditor immediately asks all the nodes in the path to submit their bitmaps. Firstly the packet loss over statement at each node is checked. Then it constructs packet loss bitmap for each hop. For packet loss on each hop, the auto correlation function is determined.

Let the bit maps of packets at each node be m1,…,mn. Firstly, the consistency for any possible overstatement of packet loss is being checked. If there is no error, then the packets at node k+1 are subsets to the packets at node k. If there is no malicious activity the report will be truthful. In the other case, if there is any malicious activity then the packets at node k+1 will be different from that of the node k. The auditor will continuously scan the bitmaps received at every node based on the report from the destination D. Once the consistencies are been checked, the DA starts working on construction of per hop packet loss bitmaps nk for mk-1. The calculation is done starting from the source node. The packets that are lost are taken into account for the calculation of nk . The packet that is lost is given ‘0’ and the packet that is successfully received is given as ‘1’. nk can be calculated by doing a bit wise complement XOR of mn-1 and mn . Let us consider a route that includes five nodes in which three intermediate nodes are present. The hops that are needed are four. Let the number of messages that are to be sent are ten.

IV. RESULTS

For M=10
Suppose that
m1=(0,1,1,1,1,1,1,1,0,1),
m2=(0,1,1,1,1,1,1,1,0,1)
m3=(0,1,0,1,1,1,1,1,0,1),
md=(0,1,0,1,1,0,1,1,0,1)
The per hop packet loss bitmaps are calculated by
n1=(0,1,1,1,1,1,1,1,0,1)
n2=(1,1,1,1,1,1,1,1,1,1)
n3=(1,1,0,1,1,0,1,1,1,1)
n4=(1,1,1,1,1,1,1,1,1,1)
Now the auto correlation function ¥k for every sequence nk=(nk1,…,nkM), k=1,…,j
¥k(i)= $\sum_{j=1}^{M-1}$ mkjmkj+i divided by M-i ,
For i=0,…, M-1; k=1,…,j.

The relative difference between ¥k and the ACF of the wireless channel fc is calculated by the auditor.

€k= $\sum_{i=0}^{M-1}$ |¥k (i) − fc(i)| divided by fc(i)

The packet losses over the Kth hop is said to be malicious or not by using the value obtained in €k. If €k >€th , then the drop is said to be malicious. €th is the threshold error. If €k <€th , then the drop is not a malicious one where €th is the threshold error.

V. CONCLUSION AND FUTURE WORK

The malicious activity is detected by using enhanced HLA scheme considering correlations of positions of lost patterns. This method is applicable for the packet drops which are highly selective and improves the network performance. The packet drops due to the errors caused by link and malicious droppings are clearly distinguishable. The malicious activity can be determined even if the source and destination are faulty. The proposed method works well if the topology changes are very less or almost constant. So, the future work can be extended to a highly dynamic environment where the topology keeps on changing. Different protocols at different layers in wireless channel respond in different manner which is not taken into account. The proposed work can be extended by studying the behaviour of various protocols for the proposed implementation.

REFERENCES

1) D.B. Johnson, D. A Maltz, and J.Broch,” DSR: The Dynamic Source Routing Protocol for multi hop wireless ad hoc networks,” in Ad Hoc Networking, MA,USA: Addison-Wesley,2001,ch.5,pp. 139-172

2) X.Y.Li, K. Moaveninejad, and O. Frieder. Regional gossip routing and wireless ad hoc networks. ACM Journal of Mobile Networks and Applications, 10(1-2): 61-77, Feb.2005.

3) R. Ramanathan and R.Rosales-hain, “Topology control of multihop wireless networks using Transmit power adjustment,” in IEEE INFOCOM,2000

4) Young-Bae Ko and Nitin H. Vaidya, “Using location information to improve routing in ad hoc networks, ” Tech.Rep ., Department of Computer Science, Texas A&M University ,1997

5) Laura Marie feeney, Bengt Ahlgren, Assar Westerlund, “Spontaneous and ad hoc networks: issues and applications” Computer and network architectures laboatory.

6) J. Erikson, m.Faloutsos, and S.Krishnamurthy. “Routing amid colluding attackers” 2007.

7) H. Shacham and B. Waters. Compact proofs of irretrievability. Crtyptologyeprint Archive, Report 2008/073, 2008. http://eprint.iacr.org/.

8) S. Vasundra et.al , CSE, JNTUACEA, " An Efficient Protocol for Secure communication in Wireless Adhoc Networks" , Volume 3, Issue 12 December 2014.

9) M. Bellare and O.Goldreich. "On defining proofs of knowledge." In Advance in Cryptology- Crypto '92 ,volume 740 of Lecture Notes in Computer Science, pages 390 -420. Springer- verlag, 1992.

10) S. Marti, T. Giuli, K. lai, and M. Baker, "Mitigating routing misbehaviour in mobile ad hoc networks," in Proc. Of the sixth Annual International conference on Mobile Computing and Networking(MobiHoc), Boston, MA, USA, August 2000.

11) M. Bellare and P. Rogaway. The Exact Security of Digital Signatures: How to sign with RSA and Rabin . In U.Maurer, editor , proceedings of Eurocrypt ,96 , volume 1070 of LNCS , pages 399-416. Springer-Verlag ,1996.

12) S. Vasundra et.al, CSE , JNTUACEA, " Automated Functional Test Case Prioritization for Increased Rate of Fault Detection" , International journal for Innovative Research in Science and Technology, Volume 1, Issue 7, December 2014, ISSN : 2349-6010

Authors profile:

K. Hima Bindu, received B.Tech degree in Computer Science and Engineering from Sri Venkateswara University college of Engineering, tirupati, A.P, India, during 2009 to 2013. Currently pursuing M.Tech in Computer Science(Computer Science) from JNTUA College of Engineering, Anantapuramu, A.p, India, during 2014 to 2016.Her area of interests is Wireless Adhoc Networking.

Dr. S. Vasundra, presently working as a Professor and Head of the Department CSE, JNTUACEA. She completed her Ph.D from JNTUA University Anantapuramu, M.Tech from JNTUA and B.E from VTU. She is having 17 years of teaching experience and 5 years of research experience. Published 36 papers in various international journals and 21 National and international conferences. Her area of interest includes MANETS, Cloud Computing, Algorithms, Data Structures and Distributed Computing.

.