International Journal of Security and Its Applications
Vol. 10, No. 4 (2016), pp.63-70
http://dx.doi.org/10.14257/ijsia.2016.10.4.07

Improvement of Trust and Reputation using Intrusion Detection and Authentication in Ad Hoc Networks

Gulshan Kumar, Rahul Saha*, Mritunjay Kumar Rai

Lovely Professional University, Phagwara, Punjab, India
rahaaot@gmail.com

Abstract

The indefinite need of dynamic environment has always imposed a concern on ad hoc networks and its application. It is often found that the internal nodes in such infrastructureless network are compromising with the trust factor to forward the packets and are able to exploit the trust to create different types of attacks such as black hole, worm hole, DDoS etc. The recent literature survey in this line of study gives an impression to the fact that the trust for the internal nodes in the networks has been emphasized less while designing any security approach for the routing protocols. Besides, the concept of watchdog/pathrater has been considered to be an inefficient if used alone. Therefore, in this paper, we have proposed an algorithm using intrusion detection and authentication method to provide enough trust in the routing path. The algorithm is having two layer of security aspect: watchdog-pathrater is used as the first layer along with a threshold value and secondly, end-to-end authentication is used to maintain the trust among the nodes in the network. The results are simulated in Network Simulator-2 (NS2). The results of the simulation show that the proposed algorithm minimizes the attacks in routing path. We have also compared our proposed algorithm with the two existing algorithm recently identified in the literature. The comparison also depicts the fact of the efficiency of our algorithm.

Keywords*: authentication, watchdog, pathrater, reputation, trust, keys*

1. Introduction

The dynamic necessity of the applications makes the ad hoc networks grooming day by day. Mobile devices are used for ad hoc networks and create a network environment which is not having any predefined infrastructure. A number of challenges are faced by these networks and security issues [1] are one of them. To tackle this problem secure access architecture for Mobile Ad-hoc Networks was explained in [2, 3]. But still this problem is not totally solved. In [4], three dimensions of secure communications are suggested. There are many other solutions exist to provide security [5] to the communications taking place through ad hoc networks. A recommendation exchange protocol was proposed in [6] to develop trust between the communicating nodes. So providing security to ad hoc communication is a need of every moment. In this paper another approach of developing trust and reputation is being proposed with the help of watchdog/ pathrater concept. [1]

Misbehaving nodes not only occur for a malicious attack, it can also be for some obvious reasons such as network traffic, overloading of packets, software issues and *etc*. to monitor the nodes in all aspects. Each node is having a watchdog and a pathrater [7]. Watchdog verifies if the node is forwarding packets to its neighbors or not. Each time a

Rahul Saha is the corresponding author.

ISSN: 1738-9976 IJSIA

node fails to forward packet, watchdog increments the failure tally. If the value of the tally increases above the threshold value it may be considered as maliciousness of the node. The pathrater then rates this path with a value and informs other nodes to avoid route through that particular path. Apart from using watchdog-pathrater, the concept of Authenticated Routing for Ad hoc Networks (ARAN) [8] is also merged.

ARAN uses cryptographic certificates. These certificates can provide authentication, integrity and non-repudiation simultaneously. For the certificates, it has to use trusted certificate server S_T whose public key is known to all other valid nodes or servers (in case of distributed servers). ARAN consists of a preliminary certification process followed by a route instantiation process that guarantees end-to-end authentication. Though there are many secure routing protocols which may use of such certificates, but they do not consider the distribution of these certificates and public key infrastructure while, ARAN seems to be expensive as it accounts in the cryptographic key distribution. Keys are basically generated in prior and are exchanged with an out-of-band (not the data communication bandwidth) relationship between the S_T and each node in the topology.

2. Related Work

The authors in the paper [9] have proposed a hybrid intrusion detection system with two layers. The first layer comprises of misuse detector to detect the known attacks. The second layer consists of anomaly detector to detect the unknown attacks. The misuse detector uses random forest classifier and the anomaly detector uses bagging technique and one class support vector machine classifiers. The proposed approach is able to detect the zero-day attacks too along with the known attacks. The detection rate improvement is 18.37%. Another hybrid approach has been shown by the authors in the paper [12]. The research work describes about a hybrid intrusion detection technique where three types of data mining techniques are in use, namely: k –means, k nearest neighbors and decision table majority. This approach can detect and classify the intrusions in four categories: remote to local, denial of service, probe and user to root.

The authors in the paper [10] have shown a novel approach of outlier detection for intrusion detection purposes. Neighbourhood outlier factor is used here for the detection of anomaly dataset and distributed approach is also followed in this concept. The proposed technique is able to detect the attacks efficiently but needs a strict training model which further creates overhead. The work done by the authors in [11] shows a review of the existing intrusion detection methods. The review of the methods has been done with respect to data mining techniques.

A light weight intrusion detection system called ELIDV has been introduced in paper [13]. The authors have executed he proposed system for vehicular network against three types of attacks as denial of service, integrity target and false alert generation. In this approach, number of intrusion detection agents is counted, then some rule based policies are executed and finally Vehicle's Behavior Evaluation Protocol (VBE) is implied to calculate the trust level or notifying the malicious level. EAACK [14] has been designed to eliminate the drawbacks of the watchdog process for intrusion detection. It comprises of three parts: acknowledgement, secure acknowledgement and misbehavior reporting authentication. The authors have also used DSA and RSA for digital signature purpose and it has been found that DSA is having better efficiency as compared to RSA with respect to overhead. A trust based intrusion detection system has been shown by the authors in paper [15]. They have calculated trust as the weighted sum of direct evaluation of the one-hop neighboring nodes and the referencing nodes. The main disadvantage of his work that is identified is that the proposed work only considers he neighbor nodes whereas the internal attacker may not be in the vicinity of one hop rather than with multiple hops. In the paper [16] the authors have proposed an efficient intrusion detection approach for AODV routing mechanism. Their approach uses a fine state machine to

specify the routing behaviour and also deploys distributed monitors. This approach can also detect the intrusion which requires more than one hop information.

All these recent approaches mentioned above considers in detecting the attacks providing some detection method. But, the aspect of the internal attacker and the trust and reputation of the nodes has been not addressed well. Therefore, in the following section we have addressed this issue and proposed the approach of using watchdog/pathrater and end-to-end authentication.

3. Proposed Idea

In the proposed approach, we have used the concept of watchdog and pathrater to create reputation and trust, besides ARAN is used to provide authentication and other security services required and also to prevent some the attacks which are based upon authentication process.

Our approach has an initialization intrusion detection level before the original data transmission begins. This will be done by watchdog-pathrater. Each node is having watchdog and pathrater. Watchdog verifies if a node forwards packets or not. Each time a packet is forwarded, pathrater will increase a trust value (T-value) by 1. The threshold of T-value must be predetermined. If T-value of a particular node is too much higher than the threshold it can be considered as a DDoS attack or flooding. Even, if the value is too much less than the threshold, it can also be considered as a packet-dropping attack. So, considering both the upper bound and lower bound of the threshold, we can avoid such attacks. T-value in a particular range will define the reputation of the node in the network which can be further considered for data transmission.

There may be circumstances, even after having this initial phase of intrusion detection, a malicious node spoof identity of an original node and create wormhole or other authentication spoofed attacks. Such attacks can be avoided by applying end-to-end authentication protocol as done in ARAN.

An efficient routing can be considered when a message transmission is done with security, authenticated and timely manner. ARAN can accomplish this objective. ARAN will provide end-to-end authentication in each forwarding and neighboring nodes and ultimately reach the destination. Destination will have an algorithm to consider the path for reply with maximum hop counts rather than minimum hop counts. The route through which destination sends reply to sender back can be considered for most authenticated and responsive route to transmit. After establishing the route, data can be sent with any cryptographic encryption procedure.

4. Network Model

The network consists of a set of nodes V and a set of edges E and is represented by G= (V, E) where v_i , $v_j \in V$ and $v_i \neq v_j$ We have measure the threshold value of pathrater by the degree of connectivity of an ad hoc node. It is given as:

Threshold $_{lowerbound}$ $(a_i) = \sum e_{ij}$ where, $\forall$ i, j = 1, 2, 3…..n a_i and a_j are neighbours and connected by edge e_{ij}.

Threshold $_{upperbound}$ $(a_i)= n(n-1)/ 2$ where i= 1,2,3…….n and n is the total number of nodes in the graph.

In the second part, keys are basically generated in prior and are exchanged with an out-of-band (not the data communication bandwidth) relationship between the certificate server S_T and each node in the topology. Each node receives exactly one certificate $Cert_N$, after getting authenticated itself, as follows:

$$S_T \rightarrow Cert_N = [IP_N, K_N+, t, e] K_{ST} -$$

Where, IP_N is the IP address of a particular node, K_N+ is the public key of that node, t is the timestamp when the certificate was created and e is the expiry time of the certificate. This total certificate is digitally signed by $K_{ST}-$ which is the private key of the certificate server. All nodes must make them updated itself by having a fresh certificate always. For a sender node S we can write the above format in the following way.

$$S_T \rightarrow Cert_S = [IP_S, K_S+, t, e] K_{ST} -$$

After this certificate generation, the source node initiates a route discovery process and provides end-to-end authentication. The source node S begins this route discovery by broadcasting a route discovery packet (RDP) to its adjacent neighbors in the following format:

$$S \text{ broadcasts: } [RDP, IP_D, N_S] K_S - , Cert_S$$

where RPD is the identifier to denote the type of packet, IP_D is the IP address of intended destination D, N_S is the nonce created by the sender. These three parameters are digitally signed by the private key K_S – of the sender. $Cert_S$, the certificate received by the sender node from the certificate server is also sent with this RPD broadcasting. The nonce is used to uniquely identify that the packet is coming from source and it is incremented each time the source performs route discovery. When an intermediate receives this RDP message, it creates a reverse path back to the source from which it has received the RDP. The receiving node uses sender's public key extracted from the certificate to validate the signature and also verifies if the certificate is expired or not. It also checks the (N_S, IP_S) tuple to verify if it has already processed this RDP message. The receiving node signs the contents of the message, appends its own certificate, and forward broadcasts the message to each of its neighbors. The signature prevents spoofing attacks that may alter the route or form loops. Now suppose, a neighbor of the sender N_1 has received the RDP from the sender and after the verification and validation it has rebroadcasted to its own neighbors as:

$$N_1 \text{ broadcasts: } [[RDP, IP_D, N_S] K_S -] K_{N1} -, Cert_S, Cert_{N1}$$

Now, when a neighbor of N_2 receives this RDP message, it verifies both the signature of sender S and the signature of its upstream neighbor N_1 from where N_2 has received the RDP message. N2 then removes the signature and certificate of N_1, records N_1 as its predecessor, signs the content of the message broadcasted by sender S and further rebroadcasts in the following format.

$$N_2 \text{ broadcasts: } [[RDP, IP_D, N_S] K_S -] K_{N2} -, Cert_S, Cert_{N2}$$

Each intermediate node along the path repeats the above steps as of node N_2 which ultimately reaches to the destination node D and verified and thus, end-to-end authentication provided by this procedure.

Now, when the RDP message is reached to the destination D it starts its function. It selects the first RDP received and reply to that RDP only. Destination D unicasts a reply packet REP back along the reverse path to source S. Assume that node N_2 first receives this REP from destination in the following format:

$$D \text{ unicasts: } [REP, IP_S, N_S] K_D - , Cert_D$$

where, REP is the identifier to denote the type of packet, IP_S is the IP address of intended source S, N_S is the nonce created by the sender. These three parameters are digitally signed by the private key K_D – of the destination. $Cert_D$, the certificate of the destination D received by the sender node from the certificate server is also attached with this REP message.

Let's N_2 is having the next hop neighbor N_1 towards source. Then N_2 unicast the REP message to N_1 in following format:

$$N_2 \text{ to } N_1: [[REP, IP_S, N_S] K_D -] K_{N2} -, Cert_D, Cert_{N2}$$

N_1 validates the signature of N_2, removes the signature and certificate of N_2, signs the REP with its private key, appends with its certificate and unicasts to next hop neighbor towards source.

$$N_1 \text{ to next hop: } [[REP, IP_S, N_S] K_D -] K_{N1} -, Cert_D, Cert_{N1}$$

Each node checks the nonce and signature of the previous hop as the REP is returned to the source. This avoids attacks where malicious nodes instantiate routes by impersonation and replay of D's message. When the source receives the REP, it verifies the destination's signature and the nonce returned by the destination. The process is shown in Figure 1.

ARAN also has the mechanism of route maintenance. When data is not received on a particular path, the particular route is deactivated. Any data received on such inactive path creates an ERR message. Nodes can also this ERR message to indicate the broken link in the network. For a route between sender S and destination D, a node N_1 generates the ERR message for its neighbor N_2 as follows:

$$N_1 \text{ to } N_2: [ERR, IP_S, IP_D, N_{N1}] K_{N1}-, Cert_{N1}$$

This message in forwarded to the source without any modification. It is extremely difficult to detect when ERR messages are fabricated for links that are truly active and not broken. However, the signature on the message prevents impersonation and enables nonrepudiation. A node that transmits a large number of ERR messages, whether the ERR messages are valid or fabricated, should be avoided.

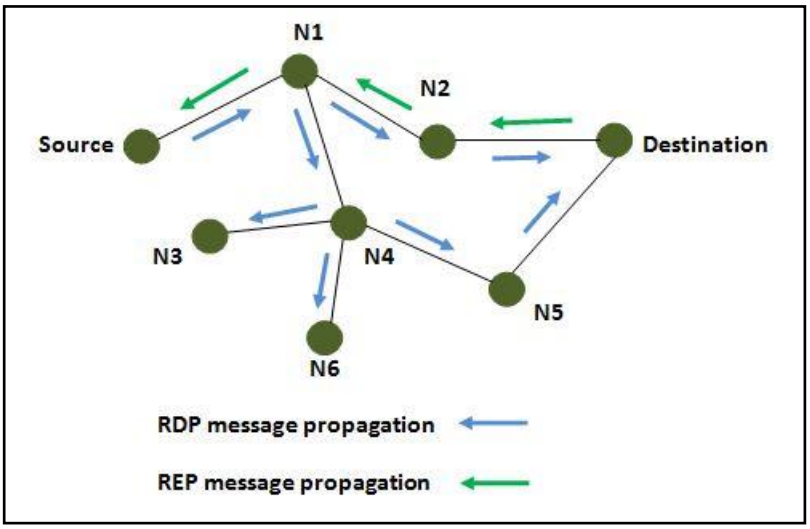

Figure 1. Basic Function of ARAN

5. Results

The proposed approach has been simulated in NS-2 simulator with the following network parameters listed in Table 1.

Table 1. Simulation Parameters

Parameter	Level
Area	1500 m X 1500 m
Speed	uniformly distributed between 0 and 20 m/s
Radio Range	300 m
Movement	uniform
MAC	Random Way Point (RWP) Model
Sending Capacity	2 Mbps
Traffic type	Constant Bit Rate (CBR)
Packet Size	128 bits
Simulation Time	1200 sec

The simulation results shown in Figure 2 and Figure 3 have been analyzed upon two parameters: mean throughput and goodput.

Mean throughput is defined as the no. of bits transferred successfully in unit time. Goodput is defined as application level throughput which calculates useful information traveled in the network per unit time. In the simulation scenario here, this parameter is measured as of a network with 100 nodes with one fourth of malicious nodes and with 30 simulation runs. Figure 4 shows that efficiency of the proposed algorithm in the terms of false positive of the maliciousness detection and the results has been compared with the recent approaches by Tesfahun et.al.[9] and Jabez et.al.[10]. The total number of nodes is varied from 10 to 100 and corresponding intrusion detection has been examined in each scenario. The comparison explains the improvement of the false positive ratio in the proposed algorithm.

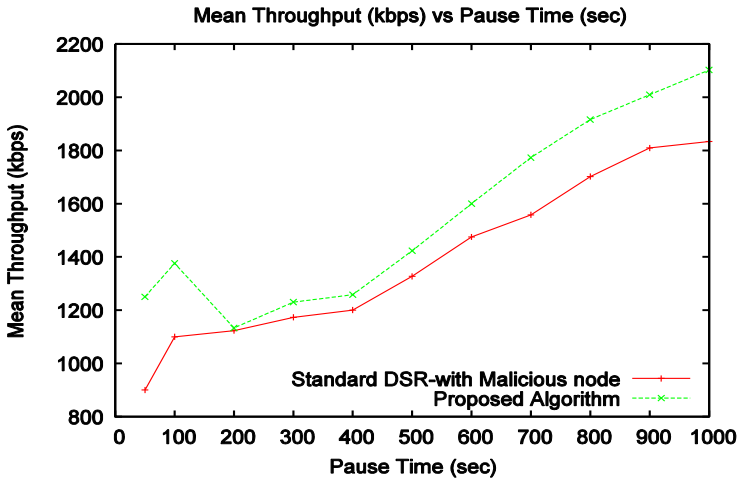

Figure 2. Mean Throughput Comparison

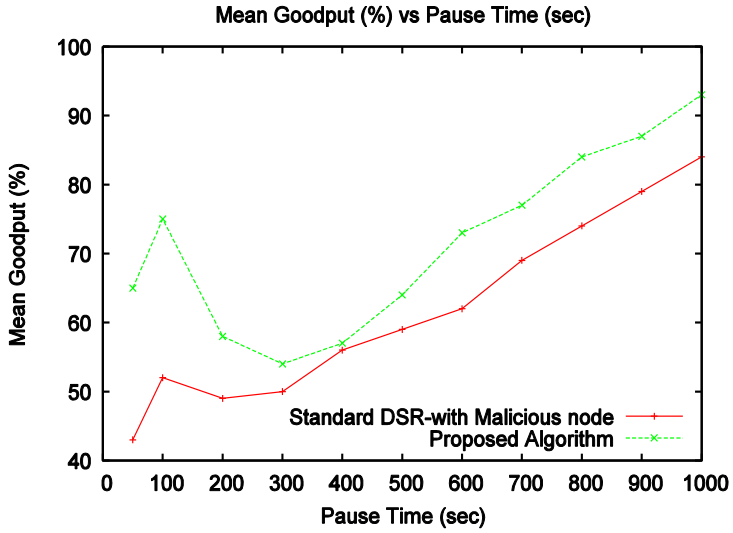

Figure 3. Goodput Comparison

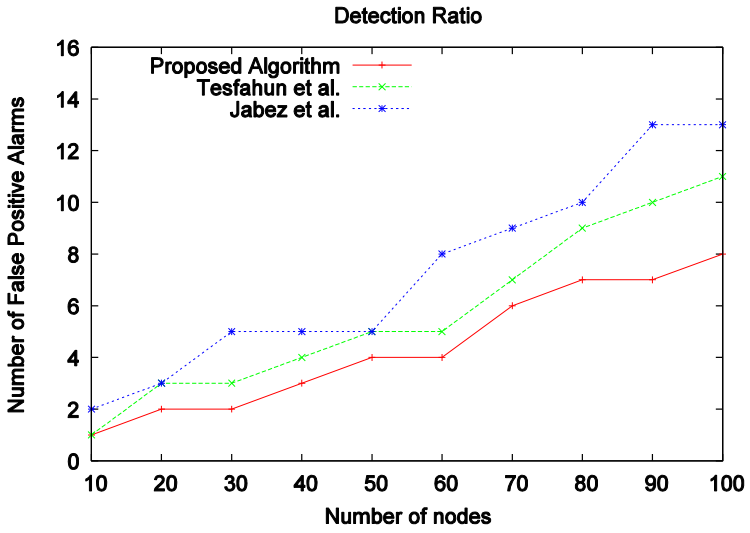

Figure 4. False Positive Comparison

6. Conclusion

Trust is an important factor in the dynamic infrastructureless environment of ad hoc networks. In this paper, the research work shown emphasizes on creating trust and reputation among the ad hoc nodes in the network. The combined approach of watchdog/pathrater and Authenticated Routing for Ad Hoc Networks (ARAN) has been proved as an efficient approach in this process. The results have been analysed thoroughly that shows a significant effect in preventing malicious attacks and improving the throughput and goodput of the network. The results also show the efficiency of the proposed algorithm as the detection rate is upto 90%.

References

[1] J Hoebeke, I Moerman, B Dhoedt, and P Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges", The Communications Network, Vol. 3, No. 3, **(2004)**, pp. 60-66.
[2] A. Bakar, I. Roslan, A. R. Ahmad, J. L. Abd Manan, "Ensuring Data Privacy and Security in MANET: Case in Emergency Rescue Mission", Proceedings of the International Conference on Information and Knowledge Management (ICIKM), Kuala Lumpur, Malaysia, **(2012)** July 24–26.
[3] Yang, H., Ricciato, F., Lu, S., & Zhang, L., "Securing A Wireless World", The Proceedings of IEEE, Special Issue on Security and Cryptography, Vol. 24, No.2, **(2006)**, pp. 443-454.
[4] V. Balakrishnan, & V. Varadharajan, "Designing secure Wireless Mobile Ad Hoc Networks", Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05), Taipei, Taiwan, **(2005)**, March 28-30**.**
[5] Amitabh Mishra, Ketan Nadkarni, Animesh Patcha, "Intrusion Detection In Wireless Ad Hoc Networks", IEEE Wireless Communications, Vol. , No. , **(2004)**, pp.48-60.
[6] P. Velloso, R. Laufer, D. D. O. Cunha, O. C. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," IEEE Transactions on Network and Service Management, Vol. 7, No. 3, **(2010)**, pp. 172-185.
[7] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proceedings of 6th Annual International. Conference on Mobile Computing and Networks, Boston, USA, **(2000)**, August 6-11.
[8] Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, "Authenticated Routing for Ad Hoc Networks", IEEE Journal on Selected Areas in Communications, Vol.23, No.3, **(2005)**, pp. 598-610.
[9] Abebe Tesfahun, D. Lalitha Bhaskari, "Effective Hybrid Intrusion Detection System: A Layered Approach", International Journal Computer Network and Information Security, Vol.7, No.3, **(2015)**, pp.35-41.
[10] Jabez Ja, Dr.B.Muthukumarb, "Intrusion Detection System (IDS): Anomaly Detection using Outlier Detection Approach", Proceedings of International Conference on Computer Communication & Convergence (ICCC 2015), Bhubneswar, India, **(2014),** December 27-28**.**
[11] Sanjay Sharma , R. K. Gupta, "Intrusion Detection System: A Review"**,** International Journal of Security and Its Applications, Vol. 9, No. 5, **(2015)**, pp. 69-76.
[12] V. I. Memon and G. S. Chandel, "A Design and Implementation of New Hybrid System for Anomaly Intrusion Detection System to Improve Efficiency", International Journal of Engineering Research and Applications, Vol. 4, No.5, **(2014)**, pp. 01-07.
[13] H. Sedjelmaci, S.M Senouci, M.A Abu-Rgheff, An Efficient and Lightweight Intrusion Detection Mechanism for Service-Oriented Vehicular Networks, IEEE, Internet of Things Journal, Vol.1, No.6, **(2014)**, pp.570-577.
[14] E. M. Shakshuki, Nan Kang; T. R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol.60, No.3 , **(2013)**, pp. 1089 – 1098.
[15] [15] Novarun Deb, Nabendu Chaki, "TIDS: Trust-Based Intrusion Detection System for Wireless Ad-hoc Networks", Proceedings of 11th IFIP TC 8 International Conference, CISIM 2012, Venice, Italy, **(2012)**, September 26-28.
[16] B. V. Ram Naresh Yadav, B. Satyanarayana, O. B. V. Ramanaiah, "Emerging Trends in Computing, Informatics, Systems Sciences, and Engineering", Edited T. Sobh and K. Elleithy, Springer, Newyork, Vol.151, **(2012)**, pp.1039-1050.

