International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 1087-1094
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

Eradication of Vulnerable host from N2N communication Networks using probabilistic models on historical data

Ms.V.M.Gayathri[1], Dr.R.Nedunchelian[2]
Research Scholar[1], Professor Department of Computer science andEngineering[2]
Saveetha University[1], Sri Venkateswara College of Engineering[2]
Vmg188@gmail.com[1], Chelian1959@gmail.com[2]

I. Abstract:

Security becomes an interesting issue in the networking field which gives wider area for the researcher to dig in. A mobile ad-hoc network is an on demand network which forms a network structure whenever it is needed. In this network, the nodes are mobile in nature which is free to move in any direction. As the nodes are moving from its position, any nodes might leave the network as well as new nodes can be entered into the network. It is hard to track the data which enters/leaves the network. Because of less authentication system, any node can enter into the network. Here in this paper, we are implementing authentication based on historical data which analyse the entire nodes in the network over a time period n. Based on the performance in that time period will be calculated and then probabilistic models will be applied to find the end result. Based on the probabilistic value conclusion can be made.

Keywords

N2N, Probabilistic, Mobile Ad-hoc Network, Eradication, Vulnerable, Authentication

II. Introduction:

A network is a collection of host which is mainly used for communication. A network structure is formed when nodes are in the particular region. The network structure varies from time to time. Since nodes are mobile in nature there is no restriction in entry and exit of the node in a network. When a node comes to the range will enter into the network, when the range is far, then the node will leave the network. A network communication is split into two categories, wired and wireless networks. A wired network is a connection between two end-users with a dedicated cable. The main disadvantage of wired network is implementation cost. Other disadvantages are portable, complexity and error recovery.

A Wireless network is of two types, they are 802.11 and ad-hoc networks. In 802.11 networks, there will be an access point to guide the communication between the networks. The connections are pre-defined one. Unlike 802.11, ad-hoc networks are on-demand networks which forms network when it is needed. Communication will also be initiated as

on-demand basis. In this network, no access point will be used. Instead of that each and every node in the network will act as router and sends the information/data to the destination node.

Ad-hoc networks are again further classified into three types. They are Mobile Ad-hoc networks, Wireless Mesh Networks and Wireless Sensor Networks. In MANET, which carries the property of ad-hoc networks in addition to that, the nodes will be mobile in nature. The main application of mobile ad-hoc network is Vehicular Ad-hoc networks. In wireless Mesh Networks, every node in the network will be connected to remaining node in the network.

In wireless Sensor Network, in addition to transmission, Sensing and aggregation are included. Internet of Things is an application of Wireless Sensor Networks. It is also called Smart systems. The device to device connection establishment will be done using these smart applications.

In this paper, the vulnerable node is being identified by n number of trail run over a particular time period 'T'. A network is formed according to the RF distance. A vulnerable node is placed in the network and communication is fully recorded. Analysis is done on the communication report. Based on the analysis, the vulnerable node is identified. The analysis is for each and every node in the network. The analysis is carried by using probabilistic method.

In section III the previous papers related will be discussed in detail. In section IV explanation of the work done is clearly explained along with algorithm. In addition to this, the detail explanation about the protocol is also discussed. In section V the results are presented and graphs are included for the better understanding. In section VI conclusion is included. In section VII references are specified.

III. Literature Survey:

[1] Explains the structure of cooperation intrusion reaction based totally multi-agent is suggest. The architecture is composed of mobile marketers. Monitor agent resides on each node and monitors its neighbour nodes. Decision agent collects facts from reveal nodes and detects an intrusion with the aid of protection policies. [2] Discussed a theoretical analysis of different security techniques of Vehicular Ad-hoc Networks has been executed which examine extraordinary schemes at distinct ranges like hardware, authentication, privacy and certification strategies.

[3] Explains the various vulnerabilities, assaults and safety mechanisms are mentioned for mobile ad hoc networks (MANETs). [4] Presents a unique idea for designing an efficient protection answer which could protect wi-fi advert hoc networks from heterogeneous attacks. This proposed Secure Routing Protocol in opposition to Heterogeneous Attacks (SRPAHA) protocol efficaciously detects and defends the collaborative malicious node without the want of high-priced signatures. The results of this paintings provide better performances as compared to current protection schemes in-phrases of security, less conversation overhead.

[5] Proves security residences of our protocols, and exhibit their effectiveness via considerable simulations and a real machine evaluation employing Epic motes and iRobot robots. [6] Identifies the malicious behavior of node by intrusion detection system with fuzzy common sense method and also to pick out the type of attacks. [7] Compares the overall performance evaluation is achieved on Adhoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), Optimized Link State Routing (OLSR) and Destination Sequenced Distance Vector (DSDV) protocols using NS2 simulator. [8] Proposed a method SSDE which is compared with existing methods, that is, full data encryption and Toss-A-Coin method with the simulation experimental setup based on NS 2.35.

IV. Implementation:

Security plays a vital role in Mobile Ad-hoc networks. Since nodes are mobile in nature, any node can come and join the network. Due to lack in security, vulnerable node can enter the network and destroys the communication in the network. In this paper, vulnerable node is inserted into the network and communication report will be taken. The conditional probability method has been applied on the report. Nodes are classified based on the results obtained.

Once the node is identified as vulnerable, the node information will be passed to other nodes in the network. The vulnerable node will be automatically deleted from the routing table. Hence the vulnerable node will be waiting for data or information since it is unaware of the deletion from the network structure. DSR Protocol is used for implementation process.

DSR:

Dynamic Source Routing (DSR) is an on-demand routing protocol. That is, it starts communicating whenever is needed. It has two phases, Route Discovery phase and Route Maintenance phase. Route discovery phase behaves somewhat similar to AODV protocol. The main difference is caching the routes. The routes are cached for future reference. In route discover phase, the shortest route will be discovered and dedicated path will be utilised for data transmission.

In Route maintenance phase, if the link between intermediate nodes to the destination node has been discarded then the node automatically communicates with the source node since the routes are cache with RERR message. Once the source node receives the message, it tries to change next least path from source to destination node.

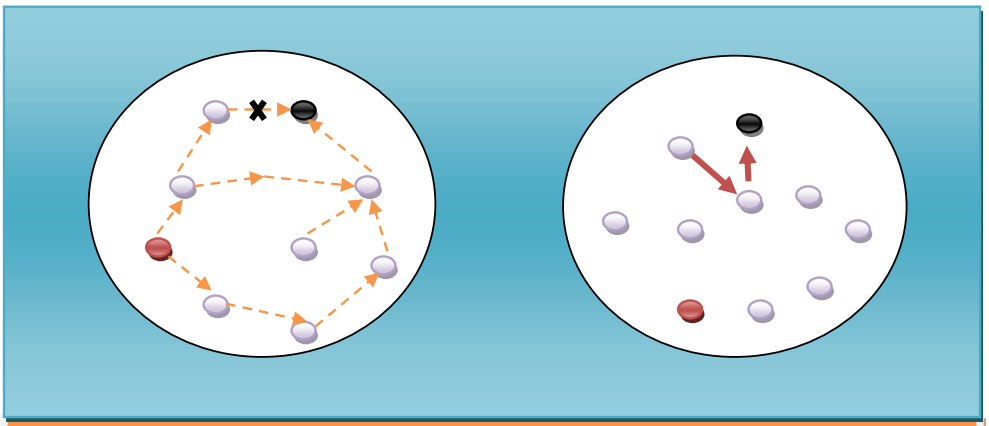

Figure 1 (a) and 1(b) explain about the route maintenance process. In figure 6 (a), black cross represents link failure between destination and other node. The intermediate node

Algorithm:

STEP 1: Define the network topology with 'n' number of nodes.

STEP 2: Add vulnerable node into the network.

STEP 3: Start the discovery phase

STEP 4: Send data/information to and from source and destination node.

STEP 5: Record the communication.

STEP 6: Identify the Trust Factor for each node in the network.

STEP 7: Run for 'n' number of simulation and compare the performance measures based on results

Trust Factor can be calculated by applying conditional probability on each and every node in the network. the conditional probability can be defined as occurrence of one event A based on the occurrence of another event B then the conditional probability can be given as,

$$P(PDR_i \cdot PDR_j) = P(PDR_i)P(PDR_j|PDR_i) = P(PDR_j)P(PDR_i|PDR_j) \quad \text{---- (1)}$$

In the above formula PDR represents performance of a node with the index i and j. The conditional probability checks on all nodes to get the performance trust factor.

$$p(pdr_n)=\sum_{i=s}^{n}\sum_{j=i+1}^{n} P(PDRi \cdot PDRj) \quad \text{---------- (2)}$$

In the above equation (2) which gives the overall dependency of a network where s represent the source node and n represents the number of nodes in the network.

V. Results:

Ns2 simulator is used for our implementation. In the below table 2 we have explained about the simulator instance of our environment. The protocol we have used is AODV. The maximum simulation time we have taken is 500 sec.

Simulator Instance	
Parameters	**Default Values**
Topology	Dynamic
Number of nodes	10-100
Transmission range	200m
MAC Protocol	802.11
Network Protocol	DSR

Packet Size	512 Byte
Packet Interval	100 packet/sec
Bandwidth	5Mbps
Simulation Time	Maximum up-to 300sec

Table 1: Simulation Parameters

In the following results, we were calculated reliability and scalability measures and then compared with Improvised algorithm implementation.

With Vulnerable node			**Without Vulnerability**		
Node	Reliability (PDR) %	Trust Factor	Node	Reliability (PDR) %	Trust Factor
1	48	0.23	1	80	0.67
2	52	0.35	2	82	0.69
3	78	0.56	3	95	0.78
4	64	0.50	4	88	0.72
5	54	0.37	5	83	0.70
6	75	0.53	6	97	0.85
7	40	0.19	7	75	0.53
8	29	0.10	8	70	0.50
9	63	0.51	9	84	0.71
10	49	0.24	10	79	0.65

Table 2: Reliability and Trust factor Value for 10 Nodes

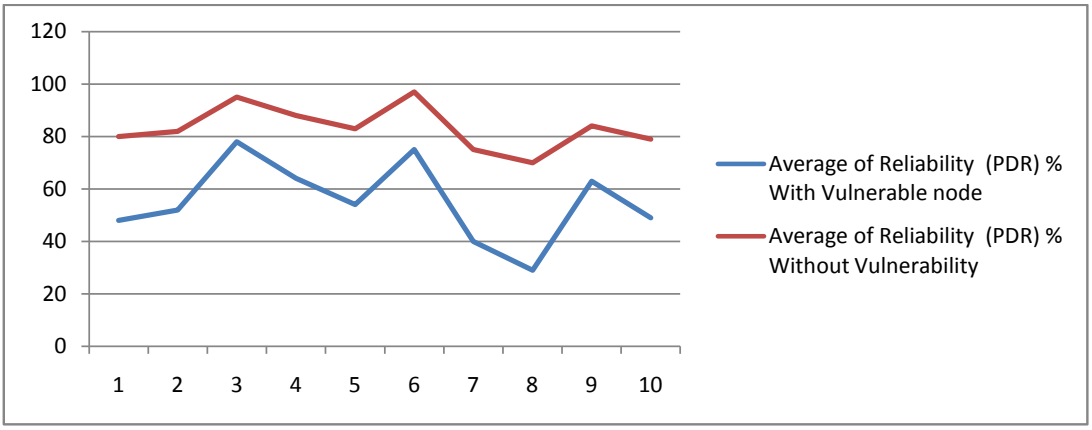

Figure 2: Reliability and Trust factor Value for 10 Nodes

In above table 2 and figure 2, the comparison between without vulnerable node and with vulnerability has been made. Performance factor in terms of reliability and trust factor of each node has been calculated. Form this we can conclude that vulnerability causes damage to the entire network as well as least trust factor is considered as most vulnerable node in the network. From the table 2, node 8 which has least performance of 29% and estimated trust factor is 0.10.

VI. Conclusion:

In recent days, ad-hoc network plays a vital role in this technological world. It has very diverse application in vehicular networks such as vehicle control, traffic analysis, route suggestion, vehicle monitoring etc. The main drawback of MANET is mobility where each node changes its location dynamically. In this paper, we implemented the trust factor for each and every node in the network for a particular time period. The data from the communication of the network will be stored and then analysis based on the performance factor. Here we took reliability of a node as a performance factor. Based on the conditional probability of two nodes the trust factor has been calculated. Form the trust factor value, the vulnerable node is being detected and communication to/from/through the node has been declined. In future, we can increase the number of vulnerable nodes in the network and compares the performance. In addition to reliability we will include power usage, scalability and synchronization as a performance factor.

VII. References:

[1] YiPing," Multi-agent cooperative intrusion response in mobile adhoc networks", Journal of Systems Engineering and Electronics, Volume 18, Issue 4, December 2007, Pages 785-794.

[2] NavjotKaur, "A Review on Security Related Aspects in Vehicular Adhoc Networks", Procedia Computer Science, Volume 78, 2016, Pages 387-394.

[3] S.Sarika," Security Issues in Mobile Ad Hoc Networks", Procedia Computer Science, Volume 92, 2016, Pages 329-335.

[4] E.Suresh Babu," Analysis of Secure Routing Protocol for Wireless Adhoc Networks Using Efficient DNA Based Cryptographic Mechanism", Procedia Computer Science, Volume 70, 2015, Pages 341-347.

[5] RaduStoleru," Secure neighbor discovery and wormhole localization in mobile ad hoc networks", Ad Hoc Networks, Volume 10, Issue 7, September 2012, Pages 1179-1190.

[6] E. VishnuBalan," Fuzzy Based Intrusion Detection Systems in MANET", Procedia Computer Science, Volume 50, 2015, Pages 109-114.

[7] S.Mohapatra," Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator", Procedia Engineering, Volume 30, 2012, Pages 69-76.

[8] AjayKushwaha," A Novel Selective Encryption Method for Securing Text Over Mobile Ad Hoc Network", Procedia Computer Science, Volume 79, 2016, Pages 16-23.

[9] Rajesh, M., and J. M. Gnanasekar. "Annoyed Realm Outlook Taxonomy Using Twin Transfer Learning." International Journal of Pure and Applied Mathematics 116 (2017): 547-558.

[10] Rajesh, M. & Gnanasekar, J.M. Wireless Pers Commun (2017),https://doi.org/10.1007/s11277-017-4565-9

[11] Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Adhoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.

[12] Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL IN HETEROGENEOUS WANET USING FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974: 2115.

[13] Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Ad hoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.

[14] Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL USING AODV PROTOCOL SCHEME FOR WIRELESS AD-HOC NETWORK." Advances in Computer Science and Engineering 16.1/2 (2016): 19.

[15] RAJESH, M. "TRADITIONAL COURSES INTO ONLINE MOVING STRATEGY." The Online Journal of Distance Education and e-Learning 4.4 (2016).

[16] Rajesh, M. "Object-Oriented Programming and Parallelism."

[17] Rajesh, M., K. Balasubramaniaswamy, and S. Aravindh. "MEBCK from Web using NLP Techniques." Computer Engineering and Intelligent Systems 6.8: 24-26.