Wireless Pers Commun (2018) 100:311–320
https://doi.org/10.1007/s11277-017-5070-x

Trust Based Detection and Elimination of Packet Drop Attack in the Mobile Ad-Hoc Networks

Vishvas Haridas Kshirsagar[1] · Ashok M. Kanthe[2] · Dina Simunic[3]

Published online: 18 November 2017
© Springer Science+Business Media, LLC, part of Springer Nature 2017

Abstract The mobile ad hoc network (MANET) is communication network of a mobile node without any prior infrastructure of communication. The network does not have any static support; it dynamically creates the network as per requirement by using available mobile nodes. This network has a challenging security problem. The security issue mainly contains a denial of service attacks like packet drop attack, black-hole attack, gray-hole attack, etc. The mobile ad-hoc network is an open environment so the working is based on mutual trust between mobile nodes. The MANETs are vulnerable to packet drop attack in which packets travel through the different node. The network while communicating, the node drops the packet, but it is not attracting the neighboring nodes to drop the packets. This proposed algorithm works with existing routing protocol. The concept of trusted list is used for secure communication path. The trusted list along with trust values show how many times node was participated in the communication. It differentiates between altruism and selfishness in MANET with the help of energy level of mobile components. The trust and energy models are used for security and for the differentiation between altruism and selfishness respectively.

Keywords Altruism · Black hole attack · Denial of service · Gray-hole attack · Mobile ad-hoc networks · Packet drop attack · Selfishness and trust

✉ Vishvas Haridas Kshirsagar
kshirsagar.vhk@gmail.com

Ashok M. Kanthe
ashokkanthe@gmail.com

Dina Simunic
dina.simunic@fer.hr

[1] G. M. Vedak Institute of Technology, Tala, Raigad, MS, India

[2] Pillai HOC College of Engineering and Technology, Rasayani, India

[3] Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb, Croatia

1 Introduction

The MANET is an own manageable network in which any node can participate in the communication. The network is working with limited resources like the strength of signal, power, etc. The nodes are communicating with each other by using routing protocols operating at different levels of the MANET. For communication between nodes, it uses insecure media channels; they fall into malicious activity. In the MANET devices act as an autonomous system, so the malicious device can join the network at any time without any notification. Once a malicious node enters in the network, much valuable information is passed to the malicious node. A malicious node may misuse that useful information.

The MANET has different denial of service attacks like gray hole attack, black hole attack and packet drop attack. In the packet drop attack, the attacker node drops all the packets passing through it similar to black hole node, but it does not attract the neighboring nodes to drop the packet.

This paper is organized as follows: Section 2 discusses the related work. Section 3 gives detailed description about proposed work. Section 4 provides simulation work. Section 5 provides comparisons between existing work and proposed work. Section 6 gives the conclusion.

2 Related Work

Neelavathy et al. [1] introduced a novel reputation based algorithm to detect the misbehaving nodes (NRMDM). NRMDM uses local reputation value. Each node maintains the reputation value of its k-hop neighborhood. It maintains reputation value of all neighboring nodes; if neighboring nodes are more then it needs more overhead. This method is excellent for small network.

Buchegger et al. [2] proposed performance analysis of the CONFIDANT reactive protocol. The protocol works as an extension to a reactive protocol. Given algorithm mainly focuses on trust relationship based on experience, observation and forwarding behavior of intermediate nodes. Given algorithm works with dynamic source routing (DSR) protocol. This protocol has primary four pillars monitor, reputation, path manager and trust manager.

Kanthe et al. [3] proposed the impact of packet drop attack and solution for the overall performance of AODV in mobile ad-hoc networks. In this paper, the reputation and trust-based mechanism is used against packet drop attack and improves the network performance in terms of throughput, packet drop rate, packet delivery ratio, normalized routing overhead and end-to-end delay. In this paper, consideration of differentiation between altruism and selfishness is missing.

Chen et al. [4] proposed trust management in mobile ad-hoc network for bias minimization and application performance maximization. It states the trust management mechanism in the MANET and its implementation to increase the performance. This approach is an integrated social and quality-of-service trust to improve the bias and performance.

Cho et al. [5] proposed on the tradeoff between altruism and selfishness in MANET trust management. In which the tradeoff between a node's individual welfare versus global well-being is considered and also identifies the best design condition of its behavior model to balance to selfish versus altruism behaviors.

3 Proposed Work

The MANET is a large open environment network. The mobile node can participate in the communication. The existing algorithms are available for mobile ad-hoc network security. Due to an open environment of MANET there is chance of malicious activity like purposefully dropping packets, traffic observation, etc. The existing algorithms for packet drop attack are based on local reputation of the node. The different reasons behind the packet drop are like power of node, network congestion, purposefully dropping the packets and queue length etc. The hard task is to differentiate the reason for dropping of packets. If the node purposefully drops packets, then it is malicious node or selfish node. When the node drops packets due to other reason; then it is not malicious node.

The proposed work has considered two concepts, namely Trust and Energy. The Mobile Ad hoc Network works on mutual trust between neighboring nodes. The communication is done in the mobile ad-hoc network with the help of intermediate nodes. The intermediate nodes may be unknown, they can be malicious nodes. The trust is major notion for the communication. Trust is mutual understanding between different nodes present in the MANET. Trust is used to identify whether the node is malicious or not. The trust management in the MANET is usually route request (RREQ) and route reply (RREP) message passing between nodes [6]. The nodes drop packets because of insufficient energy or intentionally. The energy is used to distinguish between altruism and selfish node.

3.1 Trust

The concept of trust is as a subjective degree of belief. The trust management is important to avoid the malicious activity and increase the throughput. The trust can be generated by exchanging RREQ and RREP. This proposed work deals with the trust values assigned to each node. When RREP packet gets back to the source, then source node increases the trust value by 0.1. The trust value is assigned as 0.5 of a particular node, when nodes are communicating for the first time. It is threshold value [7]. The trust value varies from 0 to 1. Every RREP has made strong relationship between a source node and its neighboring node. The source node creates a list of all nodes having a trust value greater than 0.5 and is known as Trusted List. The nodes in the trusted list have stronger relation as compare to other nodes. When source wants to communicate with any of the destination node, then source node can pick up intermediate nodes from the trusted list to establish a path. The selected path will be most secure path for the communication. The construction of trusted list is based on RREQ and RREP. Trust list along with trust value is also calculated, it shows that how many times that a node was participated in the communication. The trust value defines the strength of the relationship between the two neighboring nodes. The Trusted list decreases the overhead of detecting malicious node. Once all nodes start communicating by picking nodes form trusted list as intermediate node, the network communication will be free from malicious nodes.

3.2 Energy

The concept of trusted list is purely depending upon RREQ and RREP. The network has many problems due to which nodes are unable to send RREP. The problems may be due to congestion in the network, inefficient energy, etc. If source node does not have RREP from neighboring node, it will not add neighboring node into trusted list. There is no concept to know the reason for failure of the RREP. To differentiate between altruism and selfish node, proposed algorithm uses energy model. While generating trust in which node is not replied due to inefficient energy, that node is not entered into trusted list even though it is not a malicious node. The selfish node does not participate in the communication process so it decreases the performance of the network. Distinguish between altruism and the selfish node is done with the help of energy model. This model calculates the energy level of each node; it classifies lower energy node and higher energy node. If any node is not replying on RREQ, then it checks energy level. If energy level is lower than its threshold value then it is not considered as malicious node and if it has higher energy level then it is considered as a selfish or malicious node.

3.3 Proposed Algorithm for Trust Based Solution to Packet Drop Attack

Basically, this algorithm works on the trusted list along with trust value and energy of the mobile node. Initially all nodes trust value and energy level will be zero. All neighboring node details are stored in local storage. When any source wants to communicate with destination, it will start sending RREQ to all neighboring nodes. When requesting node gets RREP then it will add that node to the routing table and check for the trust value. Initially trust value is zero. In beginning of the communication, the trust value 0.5 is assigned when first RREP is received by the source node. Otherwise add 0.1 to pervious trust value on receiving RREP by the node and it increments up to 1. While creating a trusted list it will check for both trust as well as energy level. Trust value must be greater than 0.5 and energy levels must be above 20% of total energy of a node then source node will add it to trust list. If trust condition is true and energy level condition is false, then it will not directly declare as malicious node. Here the algorithm creates the difference between altruism and selfishness node.

The reliable flags are used while creating a trusted list. The flags help while selecting a communication path between the source node and the destination node. While selecting node from the trusted list as intermediate node, it checks for reliable flag if it is 1 then it selects otherwise it won't.

The trusted list along with trust values and energy level is used to select a secure communication path between the source and the destination. This will help in creating the difference between altruism and selfishness nodes.

This algorithm creates the trusted list. The generated trusted list contains only trusted and working energy level nodes.

```
[Initialization E (Energy Level) and T (Trust Level) to
0]
Step 1 Start (send RREQ to each neighboring node)
Step 2 Check if reply from node
If yes goto step 3
If no goto step 9
Step 3: Add details of replying node into routing table
If rt=rtable.rt_lookup(rp->rp_dst)
If yes T=T + 0.1 and E=received E
If T > 1 then T=1
If no T=0.5 and E=received E
Step 4 Check if replying node is in the trust list
If yes check E < 20 then remove from trust list
If no goto step 5
Step 5 Check replying node T and E values
If T > 0.5 && E > 20 Add to trust List and
reliable = 1
If no goto step 6
Step 6: Reset the reliable flag
reliable = 0
Step 7: Check if replying node is final destination
node
If yes do not add node to trust list
If no goto step 8
Step 8: Execute rests part of receivreply function
Step 9: Stop
```

4 Simulation Work and Result Analysis

The proposed algorithm is simulated in Network Simulator (NS-2) [8]. NS-2 is an open source network simulation tool. The 802.11 MAC layer implemented in NS-2 is used for simulation. The protocol used is AODV. The various parameters are considered to compare the results. The wireless channel type with Omni-directional antenna type is used for link. This simulation uses 802.11 MAC type. The 300×300 m^2 simulation area is used. The routing protocol is AODV protocol and simulation time is 100 ms. The two ray ground propagation model is used for simulation.

4.1 Effect of Speed of Node on Throughput

Figure 1 shows the graphs generated between the throughput and the pause time. Figure 1 shows that when the network is under attack, the average of the packet delivery ratio is 42% and when it's under attack with the solution it improved up to 80%. When we applied solution on the packet drop attack the throughput is increased because packet dropping rate is decreased. The packet dropping rate is inversely proportional to throughput. The malicious node is included in the establishment of a path. This gives a secure path for the communication.

The throughput with an attack degrades the performance of the network. The packet dropper node drops the packets if the packets come in the route. The packet dropper node does not attract the neighboring nodes. Throughput with an attack and solution improves the performance. If the packet dropper node is the busiest node in the simulation then the performance of the network is less affected due to not attracting the neighboring node to drop the packets. The packet drop attack is not as dangerous as black hole and grey hole attack because the packet drop attacker node drops only those packets which are passing through that node.

4.2 Effect of Number of Node on Throughput Delay

Figure 2 shows throughput versus number of nodes. Figure 2 shows, when the network is under attack, the average of the packet delivery ratio is 40% and when it is under the solution, it is improved up to 83%. The proposed work differentiates between altruism and selfishness nodes. When any node wants to communicate with other node, there will be a maximum number of secure next hops for the communication.

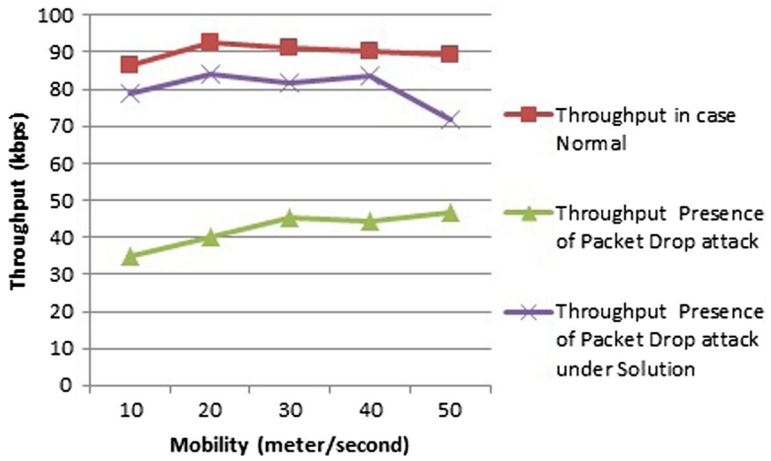

Fig. 1 Throughput versus mobility

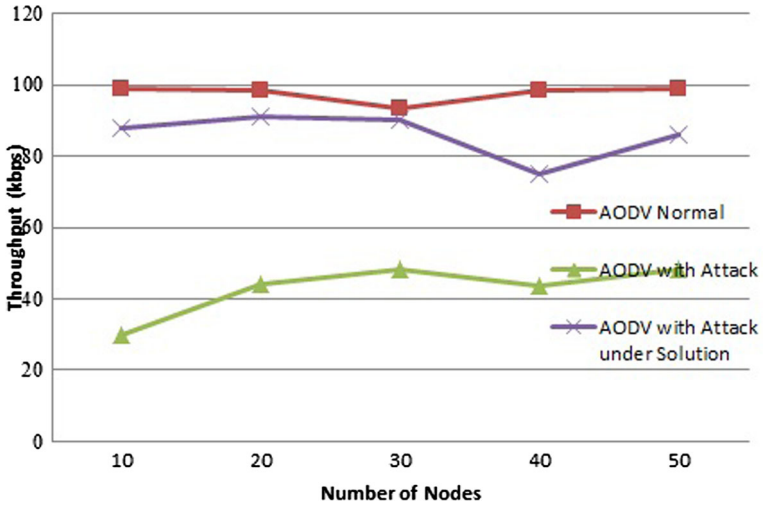

Fig. 2 Throughput versus number of nodes

5 Comparisons of Proposed Algorithm Against Existing Work

Neelavathy [1] introduced a NRMDM. NRMDM uses local values are assigned for k-hop neighboring nodes. Each node maintains all local values about its k-hop neighborhood. NRMDM solution has large overhead when large numbers of nodes are present in the network. It is suitable for small network. Buchegger [2] proposed new protocol namely the CONFIDENT protocol, which is a solution to identify the misbehaving nodes in the MANET. The overhead of computation is more because of increase in the message exchange like ALARM messages. The effect of speed of nodes on CONFIDENT protocol is affected. Each node maintains a large table for reputation. The throughput at a law pause time is less. Kanthe [3] introduces new trust based reputation algorithm against packet drop attack to detect a packet drop attack and improve the performance of the network. The concepts used in this dissertation are trust list and direct reputation. The node who does not reply to source node, it won't get added into a trust list. The node may be not replied because of energy, network issues. These existing algorithms do not work with differentiation between altruism and selfishness node. Trust based detection and elimination packet drop attack in MANET, detect the packet drop attack. This proposed algorithm works on detecting and eliminating packet drop attacks with very low overhead and end-to-end delay. Algorithm also works on the energy model to differentiate between altruism and selfishness node.

The comparative study of proposed work and existing system includes throughput, delay, overhead, technique, and packet delivery ratio and packet dropping rate [8]. The comparison of the proposed work against attack with the existing work is shown in Table 1.

Table 1 Comparisons of the algorithm against a packet drop attack with exiting work

Sr. no.	Algorithm/solutions	Protocol	Enhancement
1.	Local values assigned based on reputation [1]	DSR	In case of a large network, numbers of possible path are available. The maintenance of all path increments overhead but it decrements overall throughput of the network Local value assignment increases overhead for every node so it decreases throughput Unnecessarily caching paths and computing their local reputation values, increment end-to-end delay
2	Trust based detection of packet drop attack [2]	DSR	DSR algorithm basically works on cache memory and maintaining local reputation so it decreases overall throughput of the networks It uses ALARM packet with every RREQ and RREP messages. It consumes extra energy. Due which many nodes are unable to participate in the communication. So the less number of next hops are available for the communication. It decreases throughput of the network
3	Trust list [3]	AODV	Trust based creation of trust list with the help of RREQ and RREP gives less overhead of ALARM packet. The trust list gives more number of secure nodes for nodes for establishing the path. Throughput will be more because malicious node cannot participate in the communication The creation of trust list does not consider low energy node which is unable to send RREP to the source node. Many nodes from the network are declared as malicious node due to inefficient energy
4	Proposed work	AODV	The proposed work also depends upon the trusted list. The concept of creation of trusted list is based upon trust along with the trust value as well as the energy of the node The trusted list includes only secure node. This will help to increment in throughput of the network. This work considers energy to differentiate between altruism and selfishness node. So the maximum number of nodes can participate in the communication. It increases approximately 30–35% throughput of the network

6 Conclusion

The proposed work is identified and eliminates the malicious activity that is packet drop attack in MANET based on trust level and energy level of nodes. The method is also tradeoff between an altruism and selfishness nodes of network, which avoid getting nodes blacklisted because of their energy level. The trust based idea is better rather than cryptography, the cryptography increases overhead of computation [9].

In future, this method will be useful for survivability of the network by considering the energy level of all nodes.

References

1. Neelavathy Pari, S., & Sridharan, D. (2011). Mitigating routing misbehaviour in self organizing mobile ad hoc network using K-neighbourhood local reputation system. In *IEEE-international conference on recent trends information technology, ICRTIT*, Chennai, June 3–5, 2011.
2. Buchegger, S., & Le Boudec, J. Y. (2002). Performance analysis of the CONFIDENT protocol. In *Proceedings 3rd ACM international symposium on mobile ad hoc networking and computing (MOBIHOC 02)*, Lausanne, Switzerland, Technical Report, DSC/2001/001, June 2002.
3. Kanthe, A. M., Simunic, D., & Prasad, R. (2012). The impact of packet drop attack and solution on overall performance of AODV in mobile ad hoc networks. In *IJRTE*, ISSN:2249-8958 (Vol. 2), Dec 2012.
4. Chen, I.-R., Guo, J., Bao, F., & Cho, J.-H. (2014). *Trust management in mobile ad hoc networks for bias minimization and application performance maximization*. Elsevier B. V Journal with ISSN:1570-8705.
5. Cho, J.-H., & Chen, I.-R. (2013). *On the tradeoff between altruism and selfishness in MANET*. Elsevier B. V Journal with ISSN:2217-2234.
6. Perkins, C., Royer, E. B., & Das, S. (1999). Ad hoc on-demand distance vector routing. In *Proceeding of the 2nd IEEE workshops on mobile computing system and applications (WMCSA)* (pp. 90–100).
7. Kshirsagar, V., Kanthe, A. M., & Simunic, D. (2014). Analytical approach towards packet drop attack in mobile ad hoc networks. In *IEEE ICCIC*.
8. http://www.isi.edu/nsnam/ns.
9. Cordasco, J., & Wetzel, S. (2007). Cryptographic vs. trust-based methods for MANET routing security. In *STM*.

Vishvas Haridas Kshirsagar was born in 1989, in Anala, Dist. Osmanabad, India. He graduated in Computer Science and Engineering from B. M. I. T., Solapur University, Solapur, Maharashtra state, India in 2010. He received a Master Degree in Computer Networks from Savitribai Phule Pune University, Pune, Maharashtra State, India, in 2015. He has been working as an Assistant Professor in the G. M. Vedak Institute of Technology, Raigad under Mumbai University in India from March 2016, to present day. He has 7 years of experience as an academician in various institutes in Mumbai University and Pune University, MSBTE, in India. His research interests include mobile ad-hoc network security, protocol design and implementation.

Dr. Ashok Mallayya Kanthe was born in 1973, in Akhada Balapur, Dist. Hingoli, India. He graduated in Computer Science and Engineering from S. G. G. S. College of Engineering and Technology, Nanded, Dr. B. A. Marathwada University, Aurangabad, Maharashtra state, India in 1997. He received a Master Degree in Computer Engineering from Dr. Babasaheb Ambedkar Technological University, Lonere, Maharashtra state, India, in 2007. He has been working as an Assistant Professor in the Sinhagad Institute of Technology, Lonavala under Pune University in India from November 2007, to present day. He has 17 years of experience as an academician in various institutes in Mumbai University and Pune University in India. He is a life member of the Computer Society of India (CSI) and the International Society for Technical Education (ISTE). His research interests include mobile ad-hoc network security, protocol design and implementation.

Dr. Dina Simunic is a full professor at University of Zagreb, Faculty of Electrical Engineering and Computing in Zagreb. She graduated in 1995 from University of Technology in Graz, Austria. In 1997 she was a visiting professor in "In Wandel & Goltermann Research Laboratory" in Germany, as well as in "Motorola Inc", Florida Corporate Electromagnetic Laboratory, USA, where she worked on measurement techniques, later on applied in IEEE Standard. In 2003, she was a collaborator of USA FDA on scientific project of Medical Interference. Dr. Simunic is a IEEE Transactions on Microwave Theory and Techniques and on Biomedical Engineering and Bioelectromagnetics, Journal JOSE and a reviewer of many papers on various scientific conferences (e.g. IEEE on Electromagnetic Compatibility). She was a reviewer of Belgian and Dutch Government scientific projects, of the EU FP programs, as well as of COST_ICT and COST_TDP actions. She was acting as a main organizer of the database in the World Health Organization, for the service of International EMF Project from 2000 to 2009. From 1997 to 2000 she acted as a vice-chair of cost 244: "Biomedical Effects of Electromagnetic Fields". From 2001 to 2004, she served as vice-chair of Croatian Council of Telecommunications. In 2006, she is elected the first time and re-confirmed in 2010 as a vice-chair of Cost Domain Committee on Information and Communication Technologies (ICT). She is one of the proposer as well as a member of cost Transdomain committee. She is organizer of many workshops, symposia and round tables, as well as of special sessions (e.g., on telemedicine and intelligent transport systems during Wireless Vitae, Alborg, Denmark in 2009). She has held numerous invited Lecturers, among others at ETH Zurich, Switzerland in 1996 and US Air France, Brooks, as well as her student text for wireless communication, entitled: "Microwave Communications Basics". She is co-editor of the book "Towards Green ICT", published in 2010. She is also editor-in-chief of "Journal of Green Engineering". Her research work comprises electromagnetic fields dosimetry, wireless communications theory and its various applications (e.g.in intelligent transport system, body area networks, crisis management, security, green communications). She serves as a chair of the "Standards in Telecommunications" at Croatian standardization Institute. She serves as a member of Core group of Erausmus Mundus "Mobility for Life".