An Artificial Immune System-Based Strategy to Enhance Reputation in MANETs

Lincy Elizebeth Jim
Melbourne Institute of Technology, Australia

Mark A Gregory
RMIT, Australia

Abstract: In Mobile Ad hoc Networks (MANETs) the nodes act as a host as well as a router, thereby forming a self-organizing network that does not rely upon fixed infrastructure, other than gateways to other networks. Security is important for MANETs and trust computation is used to improve collaboration between nodes. This paper proposes an Artificial Immune System-based reputation (AISREP) algorithm to compute trust and thereby provide a resilient reputation mechanism. In this paper, the presence of selfish nodes are considered. Selfish nodes are known to enhance the reputation of their selfish peers which in turn causes packet loss. In the event of the packet being routed using the AISREP algorithm, even though the number of selfish nodes increases, this algorithm identifies the selfish nodes and avoids using the selfish nodes from the routing path thereby improving the overall performance of the network.

Keywords: MANET, Artificial Immune System, Reputation, Selfish, PAMP

Introduction

The efficiency of Mobile Ad hoc Networks (MANETs) relies on cooperation amongst the nodes to route and forward packets (Murthy & Garcia-Luna-Aceves, 1996). Therefore, it is vital to maintain effective collaboration amongst the nodes. Trust computation is used to identify the malicious or selfish nodes from the good nodes. In order to establish trust, the nodes have to be constantly monitored so that trustworthy nodes can be found to participate when routing messages. Maintaining trust between nodes in the network provides benefits to the overall network efficiency (Shaikh *et al.*, 2009). When nodes are seeking a routing path that does not have malicious, selfish or faulty nodes the computed trust values provide an important input. Trust augments traditional security by verifying that only authentic nodes are participating when routing traffic.

http://doi.org/10.18080/jtde.v7n1.176

There have been various definitions of trust proposed in the literature. The term trust has been qualitatively and quantitatively substantiated in a range of approaches based on Quality of Service (QoS), risk and other measures. Trust can also be computed using various functions such as the reputation function, by calculating direct trust and calculating trust based on recommendation. In Xiong & Liu (2003), a trust model is proposed based on filtering the badly behaving nodes from the remaining nodes in the network. The misbehaving nodes can yield a deceptive recommendation when queried and this, in turn, can lead to a variety of attacks like bad mouthing and collusion, which can hamper the trust framework. Mei *et al.* (2014) proposed a trust approach where recommendations are considered valid if a majority of nodes provide the recommendation. This is a potentially successful approach, but there is also the possibility that the majority of nodes could be colluding to launch an attack on the remaining nodes. In Buchegger & Le Boudec (2005), a trust model is proposed where trust is computed based on the prior experience of the trustee node with the node to be evaluated. This results in the use of scepticism to compute trust and circumstances may occur where the trustee node does not have prior experience with the node to be evaluated. In this paper a trust model is computed based on direct trust and indirect trust.

Background

Selfish Attacks

Safeguarding a network against attack is considered to be an important challenge today, as the potential for attack has increased significantly. Research has been carried out into packet forwarding security attacks, such as black hole (Sharma & Sharma, 2012), wormhole (Gupta & Singh, 2016), and gray hole (Sen *et al.*, 2007). It is also worth noting that trust attacks are carried out in the form of deceptive recommendations from corrupted or selfish nodes. There are other forms of attack that utilize this deceptive recommendation. The following types of attacks can be carried out:

- Bad Mouthing Attack: In this attack the selfish nodes give negative feedback about good nodes in order to tarnish their reputation. This falsified information leaves the trust management framework in a state of jeopardy (McCoy, Sicker, & Grunwald, 2007).
- Ballot Stuffing Attack: In this attack the selfish nodes collude and propagate a falsified rating to genuine nodes (Tan *et al.*, 2017).
- Incorrect Traffic Generation. This attack consists of sending false control messages. The false control messages can be sent on behalf of another node or the control messages may contain falsified routing information (Raffo, 2005).

http://doi.org/10.18080/jtde.v7n1.176

- Intelligent Misbehaviour Attack. Nodes launch intelligent attacks against the trust architecture. When the misbehaviour is insignificant to notice, it can be persistent; this attack will not be detected by traditional trust computation methods (Ishmanov & Kim, 2011).
- Time Dependent Attacks. The selfish node drops data packets at some predetermined time and behaves normally during other instances (Saha *et al.*, 2013).
- Information Disclosure. A selfish node may reveal confidential information to unauthorized nodes in the network (Basagni *et al.*, 2004).
- Eclipse Attack. In this attack the selfish node poisons the routing table of the well behaved nodes as the routing tables would contain links to a conspiracy of malicious nodes (Yih-Chun & Perrig, 2004; Schütte, 2006).

This paper considers the Ballot Stuffing Attack and Bad Mouthing Attack to evaluate the performance of the proposed approach in the midst of selfish nodes.

Artificial Immune System and Human Immune System

The immune system is a key to the defence against foreign objects or pathogens. It is necessary for the proper functioning of the immune system to maintain host well-being. The cells that play a fundamental role in this defence process are known as Dendritic Cells (DCs).

Research has been carried out into the Human Immune System (HIS) due to its distinctive ability to solve complex issues. The HIS present in the human body provides a robust defence against pathogens. The ability of the HIS to distinguish between self cells and foreign cells is noteworthy. The most important job of the HIS is to safeguard the body against pathogens. The cells, organs and tissues present in the body work in collaboration to launch a series of steps, known as an immune response, to keep the body healthy and ward off disease causing microbes.

Considerable research is being carried out in the HIS field and this knowledge is being translated into current Artificial Immune Systems (AIS) research. AISs are inspired by theoretical immunology and observed immune functions, which in turn are used to solve problems in complex domains (Abdelhaq, Hassan & Alsaqour, 2011). The evolution of AIS based research since 1990 has seen it gain prominence as a branch of computational intelligence. The four major algorithms which form the basis of AIS research are 1) Artificial Immune Networks (AIN); 2) Negative Selection Algorithm (NSA); 3) Clonal Selection (CS); and 4) Danger Theory (DT) and the Dendritic Cell Algorithm (DCA). AIS research amalgamates the principles of immunology, engineering and computer science to solve

http://doi.org/10.18080/jtde.v7n1.176

complex problems. Some of the attributes of AIS are learning, memory and pattern recognition.

The AIS based DCA is widely known for its large number of applications and well established in the literature. DT suggests that unfamiliar pathogens, which are threatening, will induce the generation of cellular molecules (danger signals) by instigating cellular stress or cellular death. These molecules are in turn perceived by Antigen Presenting Cells (APCs), critical cells that instigate an immune response.

The NSA proposed by Forrest *et al.* (1994) differentiated self cells from non-self cells based on the generation of T cells. This principle was applied to the detection of computer viruses. Since then, variations of NSA have evolved whilst keeping the original NSA principles intact.

AIS borrows its principles from HIS to solve problems in data mining, computer security, robotics and so on. DCs are antigen-presenting cells present in the HIS, where they present the antigen to the T cells, which in turn kill invaders. The features of the DCs as APCs were identified by Steinman & Cohn (1973). The state of DC is changed (Twycross & Aickelin, 2005) upon recognition of signals, such as the Pathogen Associated Molecular Pattern (PAMP) and Danger Signal (DS).

The role of the PAMP signal is noteworthy as it triggers the immune response. The DSs are released when tissue damage is suspected but they are of a lower priority than PAMP.

The DCA proposed by Greensmith & Aickelin (2008) is based on the function of DCs to investigate the state of the environment after combining various signals like DS and PAMP. The DT proposed by Matzinger (2001) forms the basis of the DCA. The DT is based on the principle that stressed cells release a DS in order to launch the immune response. The drawbacks of DT in Aickelin & Cayzer (2008) suggest the presence of an APC is fundamental for launching an immune response and the DS does not need to relate to threatening scenarios.

Proposed Reputation Model

By taking into account the trust based on a node's behaviour, there is the opportunity to consider both the direct trust and indirect trust. In direct trust, a node has to earn its reputation based on its behaviour with its immediate neighbours; and in indirect trust, the node's behaviour is calculated based on nodes other than immediate neighbours with which it would have gained reputational knowledge while routing packets for other nodes. In the same region of the MANETs, the node's behaviour is not only spatially correlated but also temporally correlated. In other words, the node's behaviour not only relates to its own history, it is also relates to other nodes in the same region. The behavioural change regularity

http://doi.org/10.18080/jtde.v7n1.176

of the node's behaviour has certain statistical characteristics that can be identified and evaluated. Based on this behaviour the direct and indirect trust value is collected by the nodes from the same region, thereby reducing data exchange among the other nodes in the network.

Computation of Trust and Reputation

In this paper, a model based on the AIS principle of DT is utilized to propose the AIS-based Reputation Algorithm (AISREP) wherein each node is modelled as a DC. Selfish nodes are detected by the DC nodes prompting the need to identify the danger by sending a DS to intermediate nodes, whereupon further action is initiated including a PAMP message. The DC nodes monitor the activity occurring in the MANET to report malicious, selfish or malfunctioning nodes. The PAMP signal is utilized here to signify the presence of a malicious, selfish or malfunctioning node in the network. Based on the aforementioned concepts a mathematical model is built.

Reputation is the quality or behaviour as seen by other nodes. Reputation is important in a MANET because the performance of the MANET depends on good behaviour by all of the nodes. Reputation is crucial because MANET functionality is not dependent on a single node. As a result, it is vital to have good reputation for all nodes and for the nodes to participate with honesty in the routing process in order to earn the good will of neighbouring nodes and, in turn, to improve network functionality and performance. A MANET with nodes that maintain a good reputation functions as expected and with improved message transmission performance. Therefore, reputation in MANETs is an interconnected system. As a result, a good reputation is able to mitigate bad mouthing by other nodes. The commendation from a reputed node is taken into consideration. The commendation from a reputed node has a higher rank based on its reputation. The node with a high reputation is given priority during trust calculations.

The concern about trustable nodes in the routing path is important as a measure of packet forwarding success. Consider the reputation for *Node a* as given in Equation (1):

$$REP_a = \frac{1}{DT}\left[\sum_{a=1}^{n-1} \frac{T_{a,n}(N_{a,n}^{S} - N_{a,n}^{PAMP})W}{N_{a,n}^{TOTAL}}\right] \quad (1)$$

where $T_{a,n}$ is the sum of direct and indirect trust, DT is trust deviation, W is the weight of the PAMP signal obtained using statistical analysis, $N_{a,n}^{S}$is the number of successful interactions between nodes a and n, $N_{a,n}^{PAMP}$is the number of times PAMP had to be sent when nodes a and n interact, $N_{a,n}^{TOTAL}$ is total number of interactions between nodes a and n.

http://doi.org/10.18080/jtde.v7n1.176

The AIS based Trust Computation model uses direct and indirect trust. Direct Trust ($T_{a,b}^{D}$) is calculated as:

$$T_{a,b}^{D} = \left(\frac{P_{a,b}}{P_{a,b} + N_{a,b}}\right) * \left(\frac{1}{N_{a,b}^{DS} + N_{a,b}^{PAMP}}\right) \quad (2)$$

Indirect Trust ($T_{a,n}^{IND}$) is calculated as:

$$T_{a,n}^{IND} = \sum_{a=1}^{n-1} \left(\frac{P_{a,n}}{P_{a,n} + N_{a,n}}\right) * \left(\frac{1}{N_{a,n}^{DS} + N_{a,n}^{PAMP}}\right) \quad (3)$$

In Equations (2) and (3), $P_{a,n}$ is the count of positive experiences (number of successful data-ack transmissions) between node *a* and node *n*, where node *n* is not an immediate neighbour of node *a;* $N_{a,n}$ is the count of the negative experiences (unsuccessful data–ack transmissions) between node *a* and node *n;* $N_{a,b}^{DS}$ is the number of times node *a* had to send a danger signal to the source due to node *b* not sending an acknowledgement; and $N_{a,b}^{PAMP}$ is the number of times PAMP had to be used during interactions between node *a* and node *b*.

Filtering AISREP Algorithm for Authentic Commendation

In this approach each node takes a role like the DCs in the HIS. In the scenario where there are no attackers, a source node sends a packet to the destination node and the intermediate nodes route traffic. As seen in Figure 1, *Node A* is the source node, *Node E* is the destination node and the intermediate nodes are *B*, *C* and *D*. The intermediate nodes respond with a Data Ack to the respective Data Send. If *Node D* is a malicious node, *D* would receive the data sent to it and might not acknowledge receipt of data causing a path disruption. The destination *Node E* would not receive the packet in this scenario or might receive a corrupt packet.

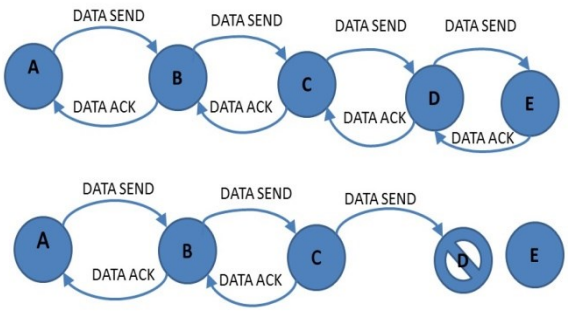

Figure 1. Routing in normal and attacker scenario

http://doi.org/10.18080/jtde.v7n1.176

In the event of the malicious *Node D* not sending a Data Ack the immediate neighbour *Node C* sends "Danger Signal (N_D)" to *Node B* in order to inform the source about the presence of a problem in the transmission path. *Node B* in turn relays this "Danger Signal (N_D)" to the source *Node A*. Once the source is informed of the presence of a problem with *Node D*, the source sends "PAMP Send (N_D)" as can be observed in Figure 2 to *Node D* and *Node D* responds with a "PAMP Ack (N_D)". PAMP is a high priority signal and it triggers an immune response; therefore, it overwrites the node buffer of the corrupted *Node D* and *Node D* is forced to acknowledge the PAMP signal. Once the presence of a defective node is identified, the routing path via this node would be avoided.

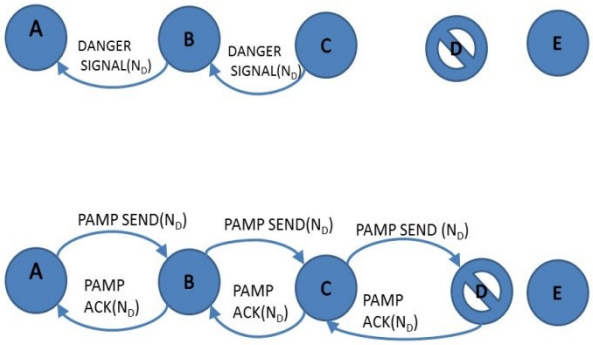

Figure 2. PAMP to confirm attacker

Simulation and Results

The Ns-3.23 simulator was used to simulate the proposed AIS based reputation mechanism (Henderson *et al.*, 2008). The pseudo-code used in the simulation is given in Table 1 and the simulation parameters are listed in Table 2.

Table 1. AISREP Pseudo Code

1. *Source node ($Node_{src}$) broadcasts Route request*
   (a) $Node_{src}$ sends data packet.
   (b)Intermediate node ($Node_{intermed}$) acknowledges data.
2. *For each intermediate set of nodes, Compute Trust (Number of DS, Number of PAMP)*
   (a) $Node_{src}$ computes Trust of $Node_{intermed}$
   (b) $Node_{src}$ sends packet to neighbor node($Node_{ngbr}$)
   (c) $Node_{ngbr}$ sends packet to the next $Node_{intermed}$
   (d) $Node_{ngbr}$ does not receive Ack
3. *$Node_{ngbr}$ sends DS to source*
4. *When $Node_{src}$ receives DS*
   (a) $Node_{src}$ sends PAMP.
   (b) $Node_{intermed}$ acknowledges PAMP.
   (c) The presence of a selfish node is detected.
5. *Compute Reputation based on the trust computed in step 2.*
6. *Isolate the selfish node.*

http://doi.org/10.18080/jtde.v7n1.176

Table 2. Simulation Parameters

Simulator	Ns-3.23
Mobility Model	Random Waypoint
Simulation Time	1000s
Number of Nodes	10-90
Routing Protocols	AODV, AISREP
Traffic Type	UDP
Network Area	300 * 1500
Mobility	6 m/s
Pause Time	0-800 s
Transmission Range	50 m

In Figure 3, the relationship between Trust and Reputation can be observed. As the Trust value, which is the combination of direct and indirect trust gathered from DC nodes, increases the reputation of the DC nodes also increases. This in turn creates an improved trust framework that can be used to identify traffic paths via the DC nodes.

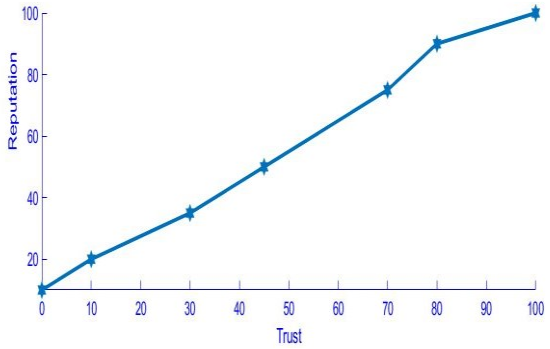

Figure 3. Reputation versus Trust

Ad hoc On-Distance Vector (AODV) (Perkins, Belding-Royer, & Das, 2003) is a reactive routing protocol for Mobile ad hoc networks. In routing protocols like AODV (Jhaveri, Patel & Jinwala, 2012) security has not been addressed and nodes are considered to be cooperative and trustworthy. The proposed approach has been compared with AODV using the performance metrics including packet delivery ratio, throughput and end-to-end delay.

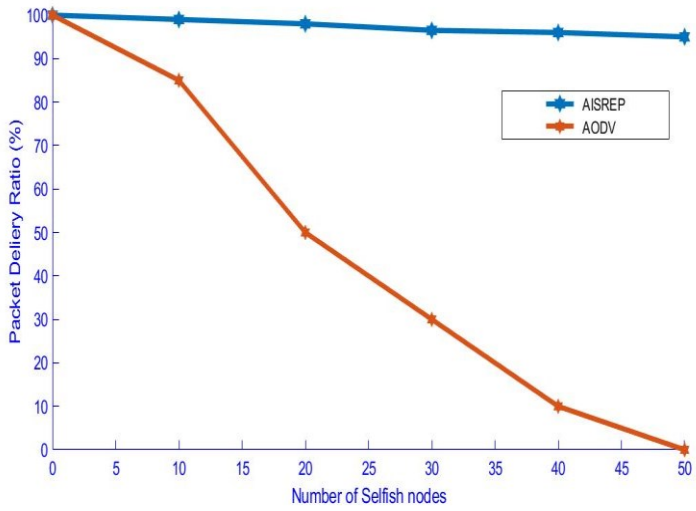

Figure 4. Packet Delivery versus Number of Selfish Nodes

http://doi.org/10.18080/jtde.v7n1.176

In Figure 4, the reputation in the presence of selfish nodes is studied. For a network that consists of non-DC nodes, it is seen that the reputation decreases for AODV nodes as they fall prey to the selfish or corrupted nodes. In the proposed AISREP, the node reputation increases in the presence of selfish nodes due to the utilization of the PAMP signal to identify and reset the selfish nodes.

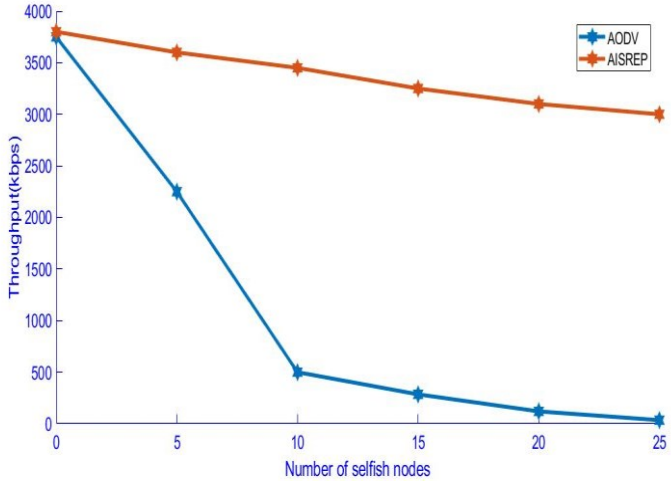

Figure 5. Throughput versus Selfish Nodes

Throughput is defined as the total number of packets delivered over the total simulation time. In Figure.5, the throughout comparison is done for AODV and the proposed AIS-based algorithm AISREP. As the number of selfish nodes increases the throughput for AODV decreases as the selfish nodes hinder the packets from reaching the destination; the selfish nodes do not facilitate the routing of packets. However, in the case of AISREP, as the number of selfish nodes increases the throughput is not drastically reduced due to the efficiency of the AISREP algorithm.

The average time taken by a data packet to reach the destination node is known as the end-to-end delay. This would include all delays that the packet encounters, such as route discovery delay and queueing delay. This metric is obtained by calculating the difference between the time *t* at which the packet was first transmitted by the source and the time *t* at which the same packet arrived at the destination.

In Figure 6, the comparison of end-to-end delay with respect to AODV and the AIS-based algorithm AISREP can be observed. As the number of selfish nodes increases, the packets sent by a source will take greater time to reach the destination node, as the selfish nodes do not allow the packet to reach the destination; whenever a packet happens to be routed by a selfish node it would take further time to reach the destination node.

http://doi.org/10.18080/jtde.v7n1.176

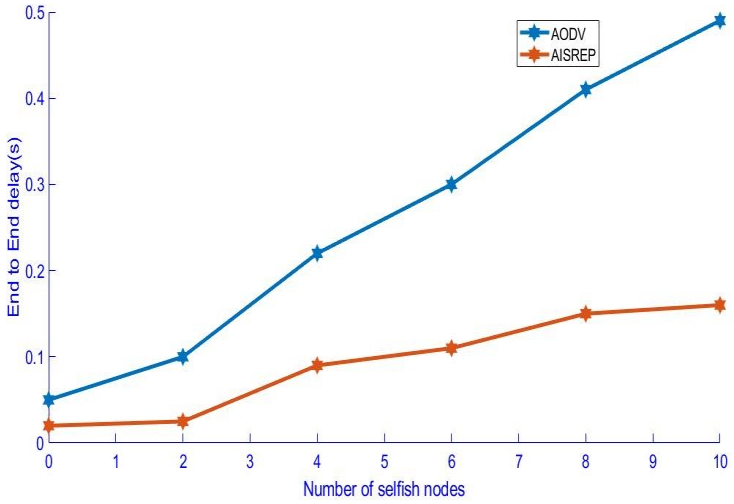

Figure 6. End-to-End delay versus Selfish Nodes

In the event of the packet being routed by nodes using the AISREP algorithm, even though the number of selfish nodes increases, this algorithm identifies the selfish nodes and avoids using the selfish nodes from the routing path. There will be delay to identify the selfish nodes but the packets eventually reach the destination with a lesser delay when compared to AODV.

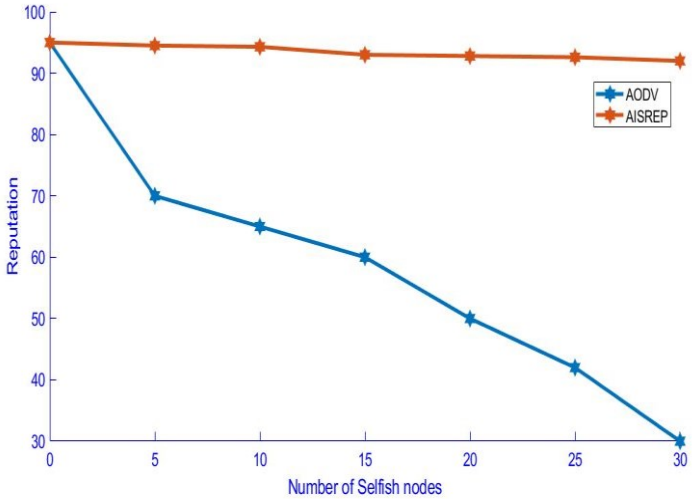

Figure 7. Reputation in Bad Mouthing attack scenario

In Figure 7, the reputation of the good nodes is considered in the Bad Mouthing attack scenario. As the number of selfish nodes increases the reputation of the good nodes goes down for AODV .This is due to the selfish nodes propagating false information. During the AISREP approach, the reputation of the good nodes is as per the expected value even in the presence of increasing selfish nodes.

http://doi.org/10.18080/jtde.v7n1.176

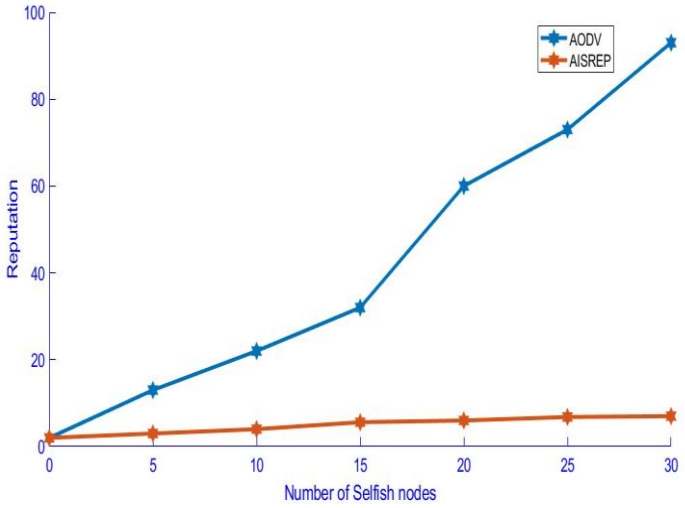

Figure 8. Reputation in Ballot Stuffing attack scenario

In Figure 8, the reputation of nodes in the Ballot Stuffing attack scenario is considered. In the scenario where AODV is used, the selfish nodes propagate false ratings about other selfish nodes, hence, as can be observed in Figure 8, the reputation value goes higher for other selfish nodes as their count increases in the network. However, in the AISREP approach, this misleading information propagated by the selfish nodes is curbed and thus the falsified information is mitigated.

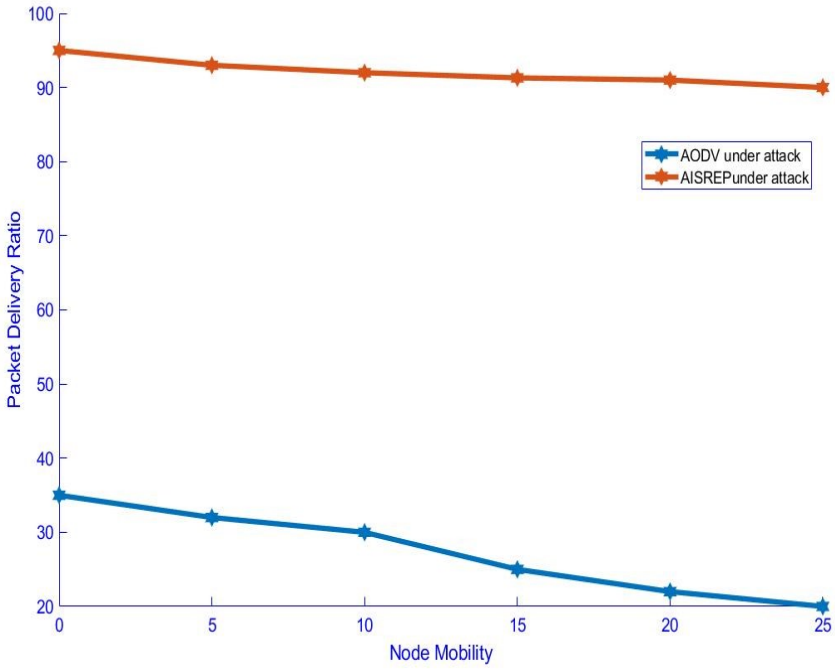

Figure 9. Packet Delivery vs Node mobility

In Figure 9, the packet delivery ratio for AODV under attack tends to decrease with increase in node mobility, whereas, for the AISREP algorithm, the packet delivery ratio increases with

http://doi.org/10.18080/jtde.v7n1.176

node mobility, as only the nodes with good reputation are chosen with the help of PAMP signals.

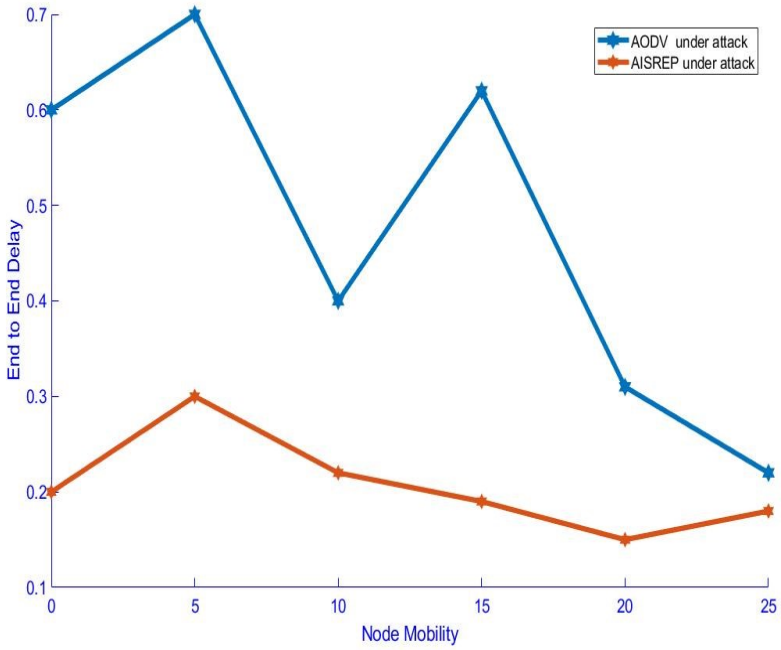

Figure 10. End-to-End Delay vs Node Mobility

In Figure 10, end-to-end delay gradually increases with increase in mobility for AODV as the corrupt nodes can cause intentional delay by not choosing to forward packets, whereas, in the AISREP algorithm due to the presence of reputed nodes, the delay encountered will be less with increase in node mobility.

Conclusion

In this paper, an AIS-based reputation mechanism is presented and the results have been analysed with the Ns-3.23 simulator. The presence of corrupt or selfish nodes is considered and the reputation mechanism depends on the direct and indirect trust commendation from the nodes in the network. The solution proposed is robust and uses AIS principles, thereby protecting the network from corrupt or selfish nodes.

This paper also considers the Bad Mouthing attack and the Ballot Stuffing attack and studies their effects on the reputation of the nodes in the network. During the Bad Mouthing attack, the selfish nodes propagate false information about good nodes but, with AISREP, the effect of false information is mitigated.

Similarly, in the case of the Ballot Stuffing attack, the selfish nodes propagate false information about other selfish nodes, claiming that they are good. In the AISREP approach, the effect of selfish nodes providing high reputations about other selfish counterparts is curbed. In some cases, the node may not be able to send an acknowledgement due to broken

http://doi.org/10.18080/jtde.v7n1.176

links through corrupt or malfunctioning nodes: therefore, there would be a situation where the commendation received from other nodes about the behaviour may not be accurate. In order to deal with this issue, a filtering algorithm is applied to aid in gaining the reputation of genuine nodes.

The simulation results obtained highlight the potential for the proposed approach as a trust framework. The AISREP approach provides improved packet delivery in the presence of selfish or corrupt nodes. In future, the AIS NSA could be utilized to enhance the trust and reputation calculations.

References

Abdelhaq, M., Hassan, R., & Alsaqour, R. (2011). Using dendritic cell algorithm to detect the resource consumption attack over MANET. Paper presented at the *International Conference on Software Engineering and Computer Systems*. https://link.springer.com/chapter/10.1007/978-3-642-22203-0_38

Aickelin, U., & Cayzer, S. (2008). The danger theory and its application to artificial immune systems. arXiv preprint arXiv:0801.3549. https://arxiv.org/abs/0801.3549

Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (2013). *Mobile ad hoc networking*. Hoboken: John Wiley & Sons. doi: 10.1002/0471656895

Buchegger, S., & Le Boudec, J.-Y. (2005). Self-policing mobile ad hoc networks by reputation systems. *IEEE Communications Magazine*, *43*(7), 101-107. https://ieeexplore.ieee.org/abstract/document/1470831

Forrest, S., Perelson, A. S., Allen, L., & Cherukuri, R. (1994). Self-nonself discrimination in a computer. *Research in Security and Privacy, 1994. Proceedings, 1994 IEEE Computer Society Symposium*. https://www.cs.unm.edu/~immsec/publications/virus.pdf

Greensmith, J., & Aickelin, U. (2008). The deterministic dendritic cell algorithm. Paper presented at the *International Conference on Artificial Immune Systems*. https://dl.acm.org/citation.cfm?id=1428224

Gupta, N., & Singh, S. N. (2016). Wormhole attacks in MANET. Paper presented at the *Cloud System and Big Data Engineering (Confluence), 2016 6th International Conference*. https://ieeexplore.ieee.org/abstract/document/7508120

Henderson, T. R., Lacage, M., Riley, G. F., Dowell, C., & Kopena, J. (2008). Network simulations with the ns-3 simulator. *SIGCOMM demonstration*, *14*(14), 527. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.415.6550&rep=rep1&type=pdf

Ishmanov, F., & Kim, S. W. (2011). A secure trust establishment in wireless sensor networks. Paper presented at the *Electrical Engineering and Informatics (ICEEI), 2011 International Conference*. https://ieeexplore.ieee.org/abstract/document/6021517

Jhaveri, R. H., Patel, S. J., & Jinwala, D. C. (2012). Improving route discovery for AODV to prevent blackhole and grayhole attacks in MANETs. *INFOCOMP, 11*(1), 1-12. http://www.dcc.ufla.br/infocomp/index.php/INFOCOMP/article/view/362/346

Matzinger, P. (2001). Essay 1: the Danger model in its historical context. *Scandinavian journal of immunology*, *54*(1-2),4-9. https://onlinelibrary.wiley.com/doi/full/10.1046/j.1365-3083.2001.00974.x

McCoy, D., Sicker, D., & Grunwald, D. (2007). A mechanism for detecting and responding to misbehaving nodes in wireless networks. Paper presented at the *Networking Technologies for Software Define Radio Networks, 2007 2nd IEEE Workshop*. https://ieeexplore.ieee.org/abstract/document/4348973

Mei, J.-P., Yu, H., Liu, Y., Shen, Z., & Miao, C. (2014). A social trust model considering trustees' influence. Paper presented at the International Conference on Principles and Practice of Multi-Agent Systems. https://link.springer.com/chapter/10.1007/978-3-319-13191-7_29

Murthy, S., & Garcia-Luna-Aceves, J. J. (1996). An efficient routing protocol for wireless networks. *Mobile Networks and Applications*, *1*(2), 183-197. https://link.springer.com/article/10.1007/BF01193336

Perkins, C., Belding-Royer, E., & Das, S. (2003). *Ad hoc on-demand distance vector (AODV) routing* (2070-1721). IETF RFC 3561. https://www.ietf.org/rfc/rfc3561.txt

Raffo, D. (2005). Security schemes for the OLSR protocol for ad hoc networks. *Université Pierre et Marie Curie*-Paris VI. https://tel.archives-ouvertes.fr/tel-00010678/

Saha, H. N., Bhattacharyya, D., Banerjee, B., Mukherjee, S., Singh, R., & Ghosh, D. (2013). A review on attacks and secure routing protocols in MANET. *International Journal of Innovative Research and Review*, *1*(2), 12-36. https://www.researchgate.net/profile/Himadri_Saha2/publication/289510067_A_REVIEW_ON_ATTACKS_AND_SECURE_ROUTING_PROTOCOLS_IN_MANET/links/568d817808aef987e56601aa.pdf

Schütte, M. (2006). Detecting selfish and malicious nodes in MANETs. Paper presented at the Seminar: *sicherheit in selbstorganisierenden netzen*, hpi/universität potsdam, sommersemester. https://pdfs.semanticscholar.org/e733/fc17534542315559f6b47906c2d2cf73390c4.pdf

Sen, J., Chandra, M. G., Harihara, S., Reddy, H., & Balamuralidhar, P. (2007). A mechanism for detection of gray hole attack in mobile Ad Hoc networks. Paper presented at the *Information, Communications & Signal Processing, 2007 6th International Conference*. https://ieeexplore.ieee.org/abstract/document/4449664

Shaikh, R. A., Jameel, H., d'Auriol, B. J., Lee, H., Lee, S., & Song, Y.-J. (2009). Group-based trust management scheme for clustered wireless sensor networks. *IEEE transactions on parallel and distributed systems*, *20*(11), 1698-1712. https://ieeexplore.ieee.org/abstract/document/4721432

Sharma, N., & Sharma, A. (2012). The black-hole node attack in MANET. Paper presented at the *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference*. https://ieeexplore.ieee.org/abstract/document/6168430

Steinman, R. M., & Cohn, Z. A. (1973). Identification of a novel cell type in peripheral lymphoid organs of mice: I. Morphology, quantitation, tissue distribution. *Journal of Experimental Medicine, 137*(5), 1142-1162. https://www.ncbi.nlm.nih.gov/pubmed/4573839

Tan, H. C., Ma, M., Labiod, H., Chong, P. H. J., & Zhang, J. (2017). A non-biased trust model for wireless mesh networks. *International Journal of Communication Systems*, *30*(9), e3200. https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.3200

Twycross, J., & Aickelin, U. (2005). Towards a conceptual framework for innate immunity. Paper presented at the *International Conference on Artificial Immune Systems*. https://dl.acm.org/citation.cfm?id=2156125

Xiong, L., & Liu, L. (2003). A reputation-based trust model for peer-to-peer ecommerce communities. *Proceedings of the 4th ACM conference on Electronic commerce*. https://dl.acm.org/citation.cfm?id=779972

http://doi.org/10.18080/jtde.v7n1.176

Yih-Chun, H., & Perrig, A. (2004). A survey of secure wireless ad hoc routing. *IEEE Security & Privacy*, *2*(3), 28-39. https://dl.acm.org/citation.cfm?id=1009287

http://doi.org/10.18080/jtde.v7n1.176