Paper No: SE-09 **Systems Engineering**

A survey on applying machine learning to enhance trust in mobile adhoc networks

G. M. Jinarajadasa*
Department of Software Engineering
Faculty of Computing and Technology
University of Kelaniya, Sri Lanka
madhushikagihani@gmail.com

S. R. Liyange
Department of Software Engineering
Faculty of Computing and Technology
University of Kelaniya, Sri Lanka
sidath@kln.ac.lk

***Abstract*: Mobile ad-hoc networks (MANETs) play a vital role in the increasingly networked world where it has many applications in plenty of important fields including military sector, business applications, social networks such as Vehicular Networks (VANETs), and other intelligent systems. Because of the dynamic nature of mobile ad-hoc networks, they are more tent to be objected to the various malicious attacks. Over the recent past decades, a certain amount of researches has been done to increase reliable and trustworthy communications in a MANET environment. Over the proposed solutions, Machine learning applications have significant results. Hence based on those, a critical analysis of existing machine learning-based trust approaches for mobile ad-hoc networks are presented here. The focus of this survey is to classify and evaluate the existing trust mechanisms and to provide guidance for future research work in the area.**

***Keywords**: Machine learning, Malicious attacks, Mobile Ad-hoc Network (MANET), Trust, Vehicular Ad-hoc Network (VANET)*

I. INTRODUCTION

Because of the increased use of mobile devices, laptops, digital devices, and other IoT (Internet of Things) devices, wireless communication mechanisms have become popular throughout the recent past years. Mobile Ad-hoc networks are one of the most used class of wireless networks which have been taken extensively for the researches in the area over the recent years.

But the major problem in the MANETs is the security issue since it is having some challenges in data transmission because of its vulnerabilities. Because of having wireless links, limited physical protection, autonomous behavior, mobility and lack of centralized infrastructure, the security of MANETs is more challenging to acquire[1].

Also, this level of vulnerability varies upon the routing mechanism as well as with the mobility models. There are a set of mobility models defined and Random Waypoint Mobility Model is the most frequently used mobility model in MANETs[2].

Specific routing protocols are defined in the context of MANETs such as AODV (Ad hoc On-Demand Distance Vector), OLSR (Optimized Link State Routing), DSDV (Destination-Sequenced Distance-Vector), BATMAN(Better Approach To Mobile Ad hoc Networking), etc[3].

Although there are a lot of routing mechanisms, confirming the security of transferring data through a MANET, it is still a major problem due to the vulnerable nature of these networks where data can be misused or compromised. Since Trust is the major component that relies upon when establishing reliable communications plenty of research works have been done considering the trust in the means of enhancing the security of MANETs.

This paper is a survey that gives a comparative explanation by a critical analysis upon the existing approaches for trust enhancement in MANETs and it especially focuses on the machine learning approaches and provides an idea for future research pathways.

Section II provides an idea about Trust in the context of MANETs and also gives some description of basic MANET challenges. The existing approaches as a whole are presented in section III and it describes guidelines for selecting the most suitable trust algorithm for MANETs based on trust properties. Existing Machine Learning approaches for MANET trust enhancement are described in section IV and provides differentiation between the machine learning techniques from different perspectives. Section V gives a summary of the presented work and the future directions for researches in the relevant area.

Fig. 1. Mobile Ad-hoc Network

II. TRUST IN MANETS

"Trust" concept is one of the most essential facts in networks when considering security services. In the context of MANETs, Trust can be declared as a node characteristic which can be a quantitative assessment of the reliability and accuracy of data received and transfer through a specific node in the perspective of the other network nodes [4][5]. Hence, a Trust Management mechanism is needed to establish security in a MANET environment by creating reliable communication links among the nodes. Establishing the trust within a MANET can be divided into several phases including calculation of trust, dissemination of trust, aggregation of trust, predicting trust and application of trust [4][5]. Figure 2 shows the primitive steps of the process of establishing trust in MANETs.

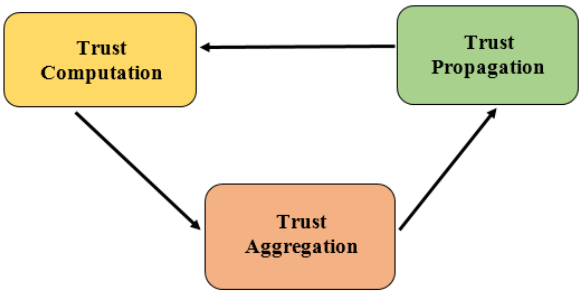

Fig. 2. Trust Establishment in a Network

A. *Challenges in MANETs*

Establishing trust or building security services in MANETs is more challenging since these ad hoc networks have a considerable amount of vulnerabilities than in the wired networks.

a) Wireless adhoc nature

MANETs do not have a central infrastructure or any other fixed infrastructure. Because of the lack of such infrastructure, nodes in a MANET play several roles including the actions of router, client and server. Also, the nodes have to communicate through multi-hops and data packets need to be travelling through different mobile nodes before arriving at their final destination. These may cause problems to arise like asymmetric links and the possibility of losing data by travelling through the malicious nodes [6][7].

b) Unreliability of wireless links

Since network connectivity is based on wireless links, MANETs are more susceptible to malicious attacks like eavesdropping, flooding, phishing, black-hole attack, wormhole attack, etc. Because of having lower bandwidth than wired networks and not wanting the physical access to make an attack, unlike in wired networks, attackers can easily exploit those features and make a severe threat to a mobile ad hoc environment [7].

c) Mobility and dynamic network topology

MANETs are consisting of a set of autonomous and highly mobile nodes where a new node/node can connect to the network constantly, and existing nodes can transit independently or leave the network. As a result of this, MANETs have a constantly changing network topology. Because of having such a dynamic environment, if some security issue occurs, it is difficult to identify the responsible nodes for such a malicious attack [6][7].

d) Energy and bandwidth restriction

MANETs have a severe resource constraints issue due to limitations in bandwidth, memory size, battery life and computational power. When considering a MANET, some or all of its nodes are relying on batteries or different exhaustible approaches for their energy. Those limitations make challenges in defining an assured routing protocol for a MANET [7][8].

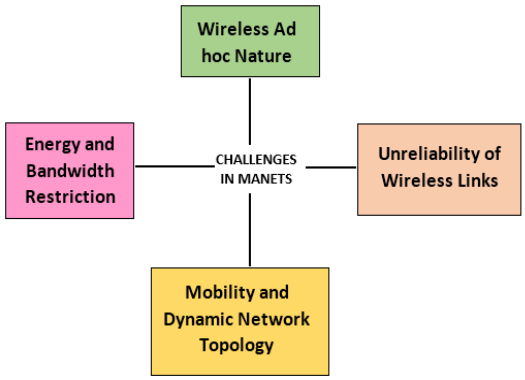

Fig. 3. Challenges in MANETs

B. *Trust properties of MANETs*

The following characteristics can be illustrated as the basic trust properties considering the unreliable and random nature of establishing communication links in MANETs.

a) Dynamicity

Due to constantly changing nature and the temptation of node failure MANET trust cannot be static, instead, it has to be dynamic which is changing accordingly [5][8].

b) Subjectivity

MANET node trust is subjective because of one node having different trust values concerning another neighbor node where it varies with the different experiences where the network topology is highly dynamic [5][8].

c) Not Inevitably Transitive

Trust in MANETs is not necessarily transitive which means having three nodes; node A, node B and node C where A trusts B and B trusts C; though it does not assure the expression A trusts C. To use the transitivity of trust, a node has to maintain 2 trust types which are direct trust and indirect trust or recommendation trust from the neighbor nodes [5][8].

d) Asymmetry

When considering the heterogeneous Mobile ad hoc network environments trust is unsymmetrical and not essentially reciprocal due to different capabilities such as a node with high computational power or battery capacity is not going to trust another node of low capabilities, but in a vice verse manner node which is having fewer capabilities is going to trust the same node with high capabilities [5][8].

e) Context dependency

MANET trust depends on context, which means different types of trust can be evaluated considering energy consumption, selfish behavior, computational power or efficiency, the occurrence frequency of malicious attacks, etc. [5][8].

III. SELECTING THE BEST ALGORITHM

When selecting the best algorithm, the above mentioned different challenges and trust properties have to be considered. Because of the physical distribution of the MANET information also have to be distributed among the nodes of the MANET. Thus the algorithms which can be distributed are

highly recommended for MANETs. The Distributed trust computing mechanisms for MANETs can be divided into 3 major types which are direct trust, indirect trust or recommendation based trust and hybrid trust[Fig.3].By considering that, plenty of researches is proposed in the area including the following approaches.

A. Swarm Intelligence

Swarm intelligence algorithms are a set of optimization algorithms that are created with the inspiration of nature; most of the time considering the behavior of social insects like ants, bees, etc. The "Antnet" and the "AntHocNet" are applications of swarm intelligence in MANETs where it utilizes the notion of Ant Colony Optimization(ACO) by finding near-best solutions to graph optimization problems[9]. Antnet and the AntHocNet are finding the near-optimal routes in a communication graph without global information. But the disadvantage of this approach is it creates additional communication overhead by the usual transferring of both 'forward ants' and the 'backward ants'[10][11]. Schoonderwoerd et al. have addressed the above-mentioned issue by proposing the solution called Ant-Based Control(ABC) which is very similar to Antnet where makes the communication overhead relatively smaller by using only the 'forward ants[12]'.

Baras and Jiang have proposed a mechanism to manage the trust in MANETs in a twofold way which is, trust document distribution and distributed trust computation. They have proposed an approach called Ant Based Evidence Distribution(ABED) for trust document distribution schemes and random graph theory to evaluate new results in the context of distributed trust computation and establishment [13].

B. Probabilistic models

A fully distributed reputation system is proposed by Sonja et al. which used a modified 'Bayesian' approach and ratings of the trust are updated upon the compatibility of information taken by third party testimonies, with prior reputation ratings in context of neighborhood recommendations or watch of the third-party testimonies and also considering the CONFIDANT routing protocol [14] [15].

An information-theoretic framework for trust modelling and evaluation in the MANETs has been proposed by Yan Lindsay Sun et al. upon some axioms. Two types of trust models have been proposed by them, which are the entropy-based trust model and the probability-based trust model. Direct trust propagation is calculated directly in the entropy-based model and the integration and the multi-path trust dissemination are calculated in the probabilistic model using the probability values [16].

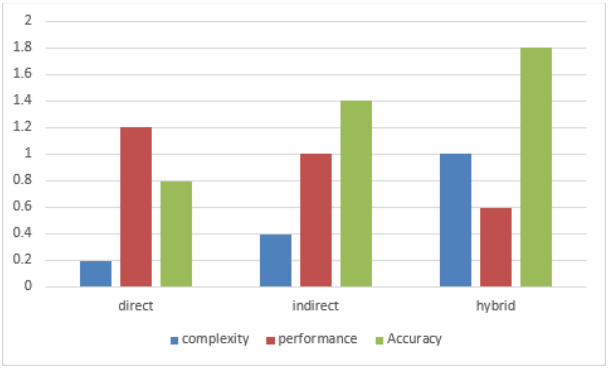

Fig. 4. Comparison of different distributed trust computing mechanisms

C. Mobile agents

In the context of networking, mobile agents can be referred to as small compositions of information or data packets that can migrate from one node to another node without any interaction with the environment. When considering the routing the applications of mobile agents such as Smart-Agents and the Ant-AODV approach updates the information about next hop or the path and find the optimal path by saving the state, transportation and resuming [17][18].

D. Machine learning approaches

Several Machine learning approaches have been proposed regarding enhancing the security of MANETs, including supervised learning, unsupervised learning, reinforcement learning and q learning. Q learning mechanism for routing enhancement has been proposed in the earliest research work in the area as well as a routing method called Q-map to secure multicast routing using the multi-agent reinforcement learning [19][20].

An approach that uses Team-partitioned, opaque-transition reinforcement learning (TPOT-RL) has been proposed for dynamic network routing which is dispersed and the implementation is not trivial. Though this achieved good results, it requires additional communication costs [21].

An implementation using Collaborative Reinforcement Learning(CRL) has been done to solve the issue of point-to-point routing in Mobile ad hoc networks [22]. A model called Trust and Q-learning based Security(TQS) is presented by Sivagurunathan et al. which can distinguish between trusted nodes and misbehaving nodes based on Q-learning [23].

A distributed reinforcement routing protocol called QLAODV (Q-Learning AODV) has been introduced to secure the information sharing in VANETs [24]. With the combination of Q-Learning and Fuzzy logic, a fuzzy constraint q learning algorithm is proposed over AODV(Ad-hoc On-Demand Distance Vector)routing protocol which is called PFQ-AODV [25].

Support Vector Machine(SVM) which is a supervised learning clustering mechanism has been applied in the area as intrusion detection agents, node clustering mechanisms and trust frameworks, which detects the misbehavior of the nodes [26][27][28].

E. Other theoretical models

Fuzzy logic-based trust computational model is presented by Ashish Kumar Jain and Vrinda Tokekar in order to enhance

the security of routing considering the AODV routing protocol. Also, they are presenting a mechanism to detect black-hole attacks in MANETs optimizing the fuzzy logic [29]. A dynamic model for predicting trust, which evaluates the trustworthiness of MANET nodes, has been proposed by Hui Xia et al. based on both historical behaviors and future behaviors where they used an extended fuzzy logic to predict future behavior. They have come up with a routing mechanism which is capable of finding the shortest path and by integrating the trust prediction model to that source routing mechanism they have introduced a novel routing protocol called Trust-based Source Routing protocol(TSR) which optimize the flexibility and feasibility of finding the shortest and optimal path [30].

Serdio et al. have used the watchdog method and the tool path-rater which runs on each node of the network where it can identify the misbehaving nodes and pick the most reliable path to transfer data [31]. CORE is a watchdog protocol-based reputation mechanism that identifies malicious nodes and enforces communication between nodes to prevent selfish behavior [32].

Further, a scalable maturity-based model for trust management which can provide recommendations about sharing data with the neighbor nodes has been proposed by Pedro et al. where they presented a protocol called Recommendation Exchange Protocol (REP) [33].

A route discovery protocol that prevents malicious attacks by providing accurate linking data has proposed by Panagiotis Papadimitratos and Zygmunt J. Haas [34].

A tool that is similar to Intrusion Detection Systems (IDS) which is separately situated on each node has been presented by the research work of A dynamic trust model for MANETs where it dynamically updates the trust value and improves the secure routing [35].

Further, ART and CAST are trusted management schemes for VANETs and context-aware trust framework for MANETs respectively [36] [37].

SEAD (Secure Efficient Ad hoc Distance Vector) is a novel routing protocol designed over the DSDV (Destination Sequenced Distance Vector) protocol that uses a one-way hash function to work against Denial-of-Service attacks and other misrouting issues [38].

Y. Shang et al have presented a heuristic search method for ad hoc networks. They have presented a distributed constraint-based routing approach which is consists of an efficient routing algorithm called CB-LRTA (Constraint-based Backpropagation LRTA) [39].

IV. MACHINE LEARNING APPLICATIONS IN MANETS

This section further describes the machine learning approaches applied to the trust enhancement of MANETs. Since mobile ad hoc networks are fully distributed systems when choosing the mechanisms also they should be distributed ones. From the above-presented paradigms Swarm Intelligence, Mobile Agents and Machine Learning Approaches are well suited to apply within MANETs. Moreover, Machine Learning algorithms are most suitable to apply within MANETs because of having the distributed manner, good prediction results, as well as the less computational power because of the collaborative manner of its help to work as a multi-agent system or to only hold the relevant part of it within each node in the network.

When compared to other distributed techniques Machine learning approaches require a medium amount of memory and computational resources. Further, the accuracy of the results is high and the initial cost and the other additional costs can be vary depending on the type of reinforcement learning technique (Table I).

TABLE I. PROPERTIES OF DISTRIBUTED APPROACHES APPLIED TO MANETS

Property	**Machine Learning**	**Swarm Intelligence**	**Mobile Agents**	**Heuristics**
Memory requirement	Medium	Medium	Low	Medium
Computational requirement	Medium	Medium	Low	Low
Flexibility to topology	High	High	High	Medium
Accuracy of results	High	High	N/A	Medium
Initial cost	High/medium	High	Low	High
Additional cost	Low	Medium	Medium	Low

A. Supervised learning approaches

Support Vector Machines are one of the supervised learning algorithms which are mainly utilized in clustering and classification purposes as well as to other data mining tasks [40].

- An application of clustering which adapts Support vector machines to classify and cluster the mobile nodes in a mobile ad hoc network into two classes as a cluster head nodes and member nodes have been proposed earlier. The classification into two groups is done by making an SVM classifier to learn the results of the WCA (Weighted Clustering Algorithm). SVM reduces the time of clustering than WCA does, especially when the mobile nodes increase [27].

- SVM based two trust approaches called SMART and Sat have been proposed upon mobile ad hoc networks for trust automation and misbehavior detection respectively. These approaches have the advantage of outperforming than the previously proposed mechanisms in the area, handling a larger fraction of adversaries. Further, these approaches are more resilient when the nodes are highly mobile as well as they can detect malicious nodes that alter their behavior over time [28] [41].

- CEAP is a multi-decision intelligence detection model that complies with the highly mobile nature of VANETs (Vehicular Ad-hoc Networks). Vehicles are classified into smart vehicles and misbehavioral vehicles by analyzing the data exchange between two vehicles with the use of SVM and they have proposed a routing protocol called VANET-QoS OLSR over the OLSR (Optimized Link State Routing) protocol [42].

B. Q learning approaches

Q-learning is one of the best reinforcement learning algorithms in which a simple and powerful way for an agent to learn optimal actions in a controlled Markovian domain environment [43]. A set of Q-learning approaches have been proposed in the area of trust enhancement in the mobile ad hoc networks.

- Boyanand and Littman have proposed a Q-routing algorithm for packet routing by embedding the reinforcement module in each node of the network. They have tested the algorithm using a network that consists of 36 nodes and the particular algorithm can find the optimal routing policies without knowing the network topology or the traffic patterns previously [19].

- The Q-MAP algorithm is a mesh-based on-demand multicast routing scheme for mobile ad hoc networks with multi-agent Q-learning. It is well adapted to the dynamic topology and using distributed agent interactions it handles the scalability and tolerates the occurring of faults. Because of this, it gives accurate results by ensuring the reliability of the resource reservation in wireless ad hoc networks [20].

- An authentication mechanism based on Q learning has been introduced in early research work, called TQS (Trust and Q-learning based Security). The particular model detects the misbehaving nodes over the AODV (Ad hoc On-Demand Distance Vector) routing protocol by using their historical behavior of data transferring. TQS is especially focusing on detecting the black hole attack which helps to improve the trust calculation by giving immediate rewards [23].

C. Dual reinforcement learning

Dual reinforcement learning implies the concepts of DQNb (Deep Q Network) and double Q learning algorithms. This is as same as Q-learning and the reward function of dual reinforcement learning algorithms uses the optimal Q-values of the next state and the previous state as well. Although this is a bit complex than the Q-learning algorithms. This Double Q-learning reduces over-estimations by dividing the target's max operation into the selection of actions and evaluations [44]. Shailesh Kumar et al. has done some evaluation on DQR (Dual Reinforcement Q-Routing algorithm) and they identified that DRQ-Routing can sustain higher network loads than Q-Routing and non-adaptive-shortest-path routing [45].

D. TPOT-RL

Team-partitioned, opaque-transition reinforcement learning (TPOT-RL) is a distributed reinforcement learning technique that has been applied within multi-agent domains. This has been achieved good results in finding the best routing path, which is non-minimal but enhancing the security and the efficiency of data sharing in the network as a whole. The implementation of the TPOT-RL is not trivial but it requires additional communication cost [21].

E. Collaborative RL

'SAMPLE' is a Collaborative Reinforcement learning-based approach that has been applied in routing as a novel routing protocol. This is also originated upon Q-Learning and it presented a reinforcement learning algorithm which is designed to solve the point-to-point routing problem. SAMPLE optimize the routing behavior and adapts to dynamic behavior by learning the variations of the network properties from routing agents. Hence this is a Q-learning approach but the only difference is it is having a decay function which is very similar to the mechanism of the Ant Colony Optimization. This approach sustains low additional cost and tolerance to the network topology changes are high [22].

TABLE II. PROPERTIES OF MACHINE LEARNING APPROACHES APPLIED TO MANETS

ML Technique	**Capturing Dynamicity**	**Additional Costs**	**Optimality of Results**
SVM	Low	High	High
Q-Learning	High	High	High
TPOT-RL	High	Medium	High
Dual RL	High	Low	High
Collaborative RL	High	Low	High

According to the above information, it is identified that more than supervised learning and unsupervised learning, reinforcement learning approaches have been used commonly since its optimality of results is high as well as it is giving the accurate predictions because of its ability to capture the dynamic behavior instead of giving predictions based upon historical values. Moreover, it can be seen that Dual RL or DRQ routing is optimal in all aspects.

V. CONCLUSION

The presented work consisted of critical analysis about applying machine learning to enhance trust in MANETs. The paper itself demonstrating machine learning approaches and other existing approaches in the research area as well. When considering all the aspects it can be seen that machine learning mechanisms outperform other mechanisms. From the approaches apart from machine learning, Swarm intelligence seems good to be applied within the MANETs since it is flexible with the high mobility of the nodes. But when comes to energy consumption it is a bit difficult to apply those swarm intelligence methods due to the energy-restricted nature of MANETs. Therefore, Machine learning techniques are far better than swarm intelligence when considering all the possible issues. Among Machine learning approaches reinforcement learning gains more suitability for applied in mobile ad hoc networks since it gives more accurate results due to the ability to capturing the dynamic behavior easily as well as no need for historical data to give predictions where it can give predictions on newly joined network node also. Among those reinforcement learning techniques, Q-learning based Dual reinforcement learning gives more accurate results than the other techniques and it is the most optimal solution when considering the other facts instead of its complexity.

Hence, considering all this information the future research work should be launch in the area of machine learning; specifically, in the area of reinforcement learning according to the presented results of early work.

REFERENCES

[1] D. Djenouri, L. Khelladi and A. Badache, "A survey of security issues in mobile ad hoc and sensor networks", IEEE Communications Surveys & Tutorials, vol. 7, no. 4, 2005, pp. 2-28. Available: 10.1109/comst.2005.1593277.

[2] L. J. Madany, M. A. Madkour, and A. H. Al-Talhi, "Characteristics of mobility models for mobile ad hoc networks," 2009 IEEE International Conference on Signal and Image Processing Applications, 2009.

[3] E. Royer and Chai-Keong Toh, "A review of current routing protocols for ad hoc mobile wireless networks", IEEE Personal Communications, vol. 6, no. 2, 1999, pp. 46-55. Available: 10.1109/98.760423.

[4] K. Govindan and P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Adhoc Networks: A Survey", IEEE Communications Surveys & Tutorials, vol. 14, no. 2, 2012, pp. 279-298. Available: 10.1109/surv.2011.042711.00083.

[5] R. Vijayan and N. Jeyanthi, " A survey of trust management in mobile ad hoc networks", Applied Engineering Research, vol. 11, no. 4, p. 2833-2838

[6] A. Forster, "Machine Learning Techniques Applied to Wireless Ad-Hoc Networks: Guide and Survey," 2007 3rd International Conference on Intelligent Sensors, Sensor Networks and Information, 2007.

[7] S. Gangwar, "Security threats in mobile ad hoc networks-A survey.", International Journal of Computer Science and Information Technologies, Vol 7, no.1, pp.74-77,2016.

[8] Cho, A. Swami and I. Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials, vol. 13, no. 4, 2011, pp. 562-583. Available: 10.1109/surv.2011.092110.00088.

[9] M. Dorigo, M. Birattari and T. Stutzle, "Ant Colony Optimization", IEEE Computational Intelligence Magazine, vol. 1, no. 4, 2006, pp. 28-39. Available: 10.1109/ci-m.2006.248054.

[10] G. Di Caro and M. Dorigo, "AntNet: Distributed Stigmergetic Control for Communications Networks", Journal of Artificial Intelligence Research, vol. 9, 1998, pp. 317-365. Available: 10.1613/jair.530.

[11] G. Di Caro, F. Ducatelle and L. Gambardella, "AntHocNet: an adaptive nature-inspired algorithm for routing in mobile ad hoc networks", European Transactions on Telecommunications, vol. 16, no. 5, 2005, pp. 443-455. Available: 10.1002/ett.1062.

[12] R. Schoonderwoerd, O. Holland, J. Bruten and L. Rothkrantz, "Ant-Based Load Balancing in Telecommunications Networks", Adaptive Behavior, vol. 5, no. 2, 1997, pp. 169-207. Available: 10.1177/105971239700500203.

[13] J. Baras and T. Jiang, "Cooperative games, phase transitions on graphs and distributed trust in MANET," 2004 43rd IEEE Conference on Decision and Control (CDC) (IEEE Cat. No.04CH37601), 2004.

[14] S. Buchegger and J. Le Boudec, " A robust reputation system for mobile ad-hoc networks ", (No. REP_WORK), 2003.

[15] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the CONFIDANT protocol," in Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing - MobiHoc 02, 2002.

[16] Yan Lindsay Sun, Wei Yu, Zhu Han and K. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks", IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, 2006, pp. 305-317. Available: 10.1109/jsac.2005.861389.

[17] E. Bonabeau, S. Guérin, D. Snyers, P. Kuntz and G. Theraulaz, " Routing in telecommunications networks with ant-like agents ", in International Workshop on Intelligent Agents for Telecommunication Applications, Springer, Berlin, Heidelberg, pp. 60-71.

[18] S. Marwaha, C. K. Tham, and D. Srinivasan, "Mobile agents based routing protocol for mobile ad hoc networks," Global Telecommunications Conference, 2002. GLOBECOM 02. IEEE, 2002.

[19] J.A. Boyan and M.L. Littman,"Packet routing in dynamically changing networks: A reinforcement learning approach," 1994 Advances in neural information processing systems , 1994, pp. 671-678.

[20] R. Sun, S. Tatsumi, and G. Zhao, "Q-MAP: a novel multicast routing method in wireless ad hoc networks with multiagent reinforcement learning," 2002 IEEE Region 10 Conference on Computers, Communications, Control and Power Engineering. TENCOM 02. Proceedings., 2002.

[21] P. Stone, "TPOT-RL applied to network routing", ICML ,pp. 935-942

[22] Dowling, E. Curran, R. Cunningham and V. Cahill, "Using Feedback in Collaborative Reinforcement Learning to Adaptively Optimize MANET Routing", IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 35, no. 3, 2005, pp. 360-372. Available: 10.1109/tsmca.2005.846390.

[23] S. S, P. K and T. A, "Authentication Using Trust to Detect Misbehaving Nodes in Mobile Ad hoc Networks Using Q-Learning", International Journal of Network Security & Its Applications, vol. 8, no. 3, 2016, pp. 47-64. Available: 10.5121/ijnsa.2016.8304.

[24] C. Wu, K. Kumekawa and T. Kato, "Distributed Reinforcement Learning Approach for Vehicular Ad Hoc Networks", IEICE Transactions on Communications, vol. 93-, no. 6, 2010, pp. 1431-1442. Available: 10.1587/transcom.e93.b.1431.

[25] C. Wu, S. Ohzahata and T. Kato, "Flexible, Portable, and Practicable Solution for Routing in VANETs: A Fuzzy Constraint Q-Learning Approach", IEEE Transactions on Vehicular Technology, vol. 62, no. 9, 2013pp. 4251-4263. Available: 10.1109/tvt.2013.2273945.

[26] H. Deng, Q.-A. Zeng, and D. Agrawal, "SVM-based intrusion detection system for wireless ad hoc networks," 2003 IEEE 58th Vehicular Technology Conference. VTC 2003-Fall (IEEE Cat. No.03CH37484), vol. Vol. 3, 2003, pp. 2147-2151.

[27] H. Chen, R. Du, P. Li,and X. Li, "Clustering Application of SVM in Mobile Ad Hoc Network.", 2008 International Conference on Intelligent Computation Technology and Automation IEEE, 2008, pp. 924-926.

[28] Li Wenjia, Anupam Joshi, Tim Finin, "SMART: An SVM-based Misbehavior Detection and Trust Management Framework for Mobile Ad hoc Networks", MILITARY COMMUNICATIONS CONFERENCE 2011-MILCOM, 2011, pp. 1102-1107.

[29] A. Jain and V. Tokekar, "Security Enhancement of AODV Protocol using Fuzzy based Trust Computation in Mobile Ad Hoc Networks," Oriental journal of computer science and technology, vol. 10, no. 1, 2017, pp. 94–102

[30] H. Xia, Z. Jia, X. Li, L. Ju and E.H.M. Sha, "Trust prediction and trust-based source routing in mobile ad hoc networks.", Ad Hoc Networks, vol 11,no. 7, 2013, pp.2096-2114.

[31] S. Marti,T.J. Giuli,K. Lai and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks.", 6th annual international conference on Mobile computing and networking, ACM, 2000, pp. 255-265..

[32] P. Michiardi and R. Molva, "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," Advanced Communications and Multimedia Security IFIP Advances in Information and Communication Technology, 2002, pp. 107–121.

[33] P. Velloso, R. Laufer, D. O. Cunha, O. 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. Available: 10.1109/tnsm.2010.1009.i9p0339.

[34] P. Papadimitratos and Z. Haas, "Secure message transmission in mobile ad hoc networks", Ad Hoc Networks, vol. 1, no. 1, 2003, pp. 193-209. Available: 10.1016/s1570-8705(03)00018-0.

[35] Z. Liu, A. Joy, and R. Thompson, "A dynamic trust model for mobile ad hoc networks," in Proceedings of 10th IEEE International Workshop on Future Trends of Distributed Computing Systems, 2004. FTDCS 2004., 2004.

[36] W. Li and H. Song, "ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks," IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 4, 2016, pp. 960–969.

[37] W. Li, A. Joshi, and T. Finin, "CAST: Context-Aware Security and Trust framework for Mobile Ad-hoc Networks using policies," Distributed and Parallel Databases, vol. 31, no. 2, 2012, pp. 353–376

[38] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks," Ad Hoc Networks, vol. 1, no. 1, 2003, pp. 175–192.

[39] Y. Shang, , M.P.Fromherz, Y. Zhang and L.S. Crawford, "Constraint-based routing for ad-hoc networks.", Information Technology: Research and Education, in Proceedings of ITRE2003. International Conference , 2003, pp. 306-310.

[40] L.Wang , Support vector machines: theory and applications ,Vol. 177, Springer Science and Business Media., 2005

[41] S. Kumar and R. Miikkulainen, “Dual reinforcement Q-routing: An on-line adaptive routing algorithm.”, Artificial neural networks in engineering Conference, 1997, pp. 231-238.

[42] O. Wahab, A. Mourad, H. Otrok and J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks", Expert Systems with Applications, vol. 50, 2016, pp. 40-54. Available: 10.1016/j.eswa.2015.12.006.

[43] W. Li, A. Joshi, and T. Finin, “SAT: an SVM-based automated trust management system for Mobile Ad-hoc Networks,” 2011 - MILCOM 2011 Military Communications Conference, 2011.

[44] C. Watkins and P. Dayan, "Q-learning", Machine Learning, vol. 8, no. 3-4, 1992, pp. 279-292. Available: 10.1007/bf00992698.

[45] H. Van Hasselt, A. Guez, and D.Silver, Deep Reinforcement Learning with Double Q-learning, AAAI, vol. 2, 2016, p. 5.