I.J. Information Technology and Computer Science, **2014, 08, 43-50**
Published Online July 2014 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijitcs.2014.08.06

Trust Formulization in Dynamic Source Routing Protocol Using SVM

Priya Kautoo
Department of Computer Science and Engineering, UIT RGPV, Bhopal, India
Email: priyakautoo@gmail.com

Piyush Kumar Shukla
Department of Computer Science and Engineering, UIT RGPV, Bhopal, India
Email: pphdw@yahoo.com

Sanjay Silakari
Department of Computer Science and Engineering, UIT RGPV, Bhopal, India
Email: ssilakari@yahoo.com

Abstract− In an advanced wireless network, trust is desirable for all routing protocols to secure data transmission. An enormous volume of important information communicates over the wireless network using trusted dynamic routing protocol, which is the enhancement of the DSR (Dynamic Source Routing) protocol to improve trust. Previously fuzzy logic, genetic algorithm, neural network has been used to modify DSR and good result has been obtained in few performance indicators and parameters. In this work an SVM based trusted DSR have been developed and better results have been presented. This new novel on demand trust based routing protocol for MANET is termed as Support vector machine based Trusted Dynamic Source Routing protocol, performance of STDSR has been improved in term of the detection ratio (%) at different mobility and no. of malicious node variation.

Index Terms− DSR, Malicious, Prediction, Reliability, Trust

I. Introduction

With the rapid development of wireless communication devices such as mobile phones, laptops, Personal Digital Assistants (PDAs), navigators, cordless phones and gaming consoles, people mostly depend upon the wireless ad-hoc networked to the inherent vulnerability of wireless ad-hoc network [1], several new security mechanisms are required to be developed to efficiently protect them. Now a day's most of the researches are an emphasis on the network security. Recently, a few key management schemes have been proposed to ensure secure communication over MANET but these techniques are not more suitable for MANET because they required some centralized administration mechanism or trusted [2] third party to issue digital certificate or observe network traffic. The centralized trusted third party actually violates the nature of self-organization. This paper focuses on the detection of malevolent nodes on the bases of behavior of nodes in DSR routing protocol (DSR is well recognized and popular reactive protocol used in mobile ad-hoc network.) [3] with the help of support vector machine. This work can help to distinguish ''normal'' against ''intrusive'' behavior efficiently. This paper uses well-known SVM based classification algorithm and uses categorized datasets obtained from a simulated environment.

The idea of trust is started when the watchdog applied to the DSR routing protocol. Trust between the nodes can be computed by several methods such as cryptography, soft computing, and fuzzy logic prediction rules some of these methods are described in the section 3.

The experiments have been accomplished with datasets produced under numerous traffic conditions regarding the network mobility and the number of malicious nodes. This paper also represents a comparison of several DSR that provides the secure routing in MANET.

In Section 2 we present the motivation of our work. Section 3 presents an analysis of related work. Section 4 describes SVM based misbehavior detection. Section 5 explains the details of the experimental setup and Section 6 presents the results obtained. Finally, we conclude in Section 7.

II. Motivation

A. Ad-hoc Network

Mobile ad-hoc network is a decentralized and an infrastructure less type of network in which each node can communicate with every other node within the transmission range and each node in MANET [4] are mobile. In MANET when a node needs to be transmitted a packet (data/control) to another node that does not belong in its one hop neighbor, then it has to rely to the intermediate node to forward the packet to the destination this mechanism is known as multi hop. Current investigation [5-6] designates that the wireless ad hoc network is more vulnerable than the conventional wired and wireless networks due to its underlying features of open medium, dynamic network topology, limited bandwidth, distributed cooperation and limited energy resources. Thus, well-organized routing protocols [7] are

required in order to enhance the communication paths. Several routing protocols have been proposed for MANET. They are mainly classified into two categories proactive and reactive routing protocol, former is the table driven routing protocol in it all the routes to destinations or for other nodes are pre-determined and preserved by the episodic update process and in proactive routing protocol routes are created on the fly or when needed. These all protocols suffer from attacks from malicious nodes because these traditional routing protocols do not encompass any security mechanism. For securing routing in recent a new class of routing protocol has been proposed called trust based routing protocol [8].

B. Trust in Ad-hoc Network

The inherent nature of MANETs provokes the appearance of new security hazards, while some existing weaknesses in wired networks are emphasized. To secure MANET from such hazards notion of trust has come in the field of MANET security. Trust is a more complex subject in physiological environment and it is influencing of assumptions, expectations, behaviors, environments, and other factors [9].

III. Related Work

Mobile ad hoc networks show new vulnerabilities to malevolent attacks or rejection of collaboration due to their characteristics. To secure the MANET a new class of security mechanism has been proposed, which are based on trust. Several trust models have been proposed which are used in the conjunction with routing protocol.

Liu et. al. [4] has been proposed a trust model in which each node detects an attack from malicious nodes in its radio range. For this model information about the attacker is propagated through the data packet instead of control packet, thus it decreases the control packet overhead. The drawback of this model is that interrupting transmission may cause undesirable results. Xia. et. al. [2] Proposed a trust management model based on fuzzy logic, this trust model is divided into two parts: subjective trust evaluation model and trusted routing model. This model correlates the MANET network as the directed graph where each node in MANET is connected by direct link and each node assigns some weight value. Throughput of the network is increased when this model is used for trust computation. All the models described above uses single scaling factor for the calculation of trust and these all models are relay on a well define the threshold to identify the possible misbehavior. A smart attacker can easily adjust this threshold value by changing its behavior from time to time. To overcome these problems Wenjia Li [10] proposed a misbehavior detection model based on support vector machine. The support vector machine is a classifier and use to detect the misbehavior. SVM do not rely on any pre-define normal behavioral pattern, nor does it require a pre-defined threshold to discriminate regular behavior from anomalous behavior.

A. Several secure DSR routing protocol

Marti et. al. [11] has been proposed watchdog and pathrather mechanism. In this mechanism each node in the MANET network contains a watchdog which monitors the behavior of its immediate neighbor and pathrather avoid routing through malicious nodes this protocol dose nothing to penalize these nodes and suffer from a black hole attack. Ariadne [12] uses one of the following three mechanisms: shared keys between all pairs of nodes, Shared secret keys between communicating nodes combined with broadcast authentication and digital signature for authentication of the routing message. Ariadne needed some centralized authority and is not more suitable for mobile Ad-hoc network. CHENG Yong et. al. [1] proposed a trusted dynamic source routing protocol which is an extension to the DSR routing protocol. This protocol employs the idea of Trust Network Connect (TNC) to protect the MANET. TDSR uses two modules: basic DSR routing protocol and the trust model. TE-DSR has been proposed by N. Bhalaji [7] in which trust enhanced routing is applied to the basic DSR routing protocol. There are mainly three components in the TE-DSR: trust Unit, monitor and the router. Unit trust is responsible for monitoring the trust score and it is further divided into three parts: Initializer, Upgrader and Administrator. The initializer module is used to assign a trust value for new unknown mobile node in the MANET. Upgrader module is responsible for upgrading of trust. The Administer is used to store all the trust information. X. Li et. al. [13] proposed a protocol in which trust is mainly classified into three parts: node historical trust, node current trust and the route trust. Multi- criteria decision making method (like AHP theory) is used for the calculation of historical trust. There are so many trust factors that define the trust such as direct trust, recommendation, an incentive function and active degree. Node current trust is computed by the fuzzy prediction rule. By analyzing all the strength and weakness of previous trust models Xui et. al. [14] proposed trust based dynamic source routing protocol. This protocol is an extension to the FTDSR protocol. For this protocol node historical trust is calculated using the single scalar value i.e. Packet forwarding ratio (ratio of packets forwarded correctly to the total number of packets forwarded from source to destination). By applying fuzzy theory node current trust is computed.

Since malicious nodes can do great destruction to MANET routing, a great number of security solution has been proposed to identify and alleviate those misbehaviors from a variety of perspectives. Most of these previously discussed trust management techniques are based on a well-defined threshold. But it is not possible to set an appropriate threshold a smart adversary can easily adjust this threshold and for all of these methods trust is computed with single scalar parameter. All of these problems can be overcome by STDSR, which uses a support vector machine algorithm in which multidimensional Trust management scheme is applied that evaluate the trustworthiness of DSR nodes, from the multiple perspectives [15].

IV. SVM Based Misbehavior Detection

Support vector machine is the collection of supervised learning techniques which are primarily used for classification and regression analysis. It is mainly used for small sample data and it is not complex for data dimension. Therefore SVM algorithms are suitable to the characteristics of the m-dimensional heterogeneous and uneven data sets into single dimensional data sets [16]. Given a training datasets, (x_i, y_i) where x and y is the input and output space respectively and i=1 to n is the i-th dimension of trustworthiness for nodes. $y_i \in \{-1, +1\}$

It finds the hyper planes that have a maximum margin:

$$w.x = b$$

Where w is a normal vector and b is a threshold.

In order to find the optimal hyper plane, it solves following convex optimization problem,

$$min\left\{\frac{w^2}{2} + c\sum_{1=1}^{n}\xi_i\right\} \quad (1)$$

$$y_i\left(w.x_i + b\right) \geq 1 - \xi_i, \xi_i \geq 0$$

Here c is a penalty constant that control the trade off the empirical error ξ and the margin.

The equation (1) can be handled by using following Lagrange equation

$$\text{Maximize } L(\alpha_i) = \sum_{i=1}^{n}\alpha_i - \sum_{i=1}^{n}\sum_{j=1}^{n}\alpha_i\,\alpha_j\,y_i\,y_j\,K(x_j, x_i) \quad (2)$$

Subjected to $\sum_{i=1}^{n} y_i\,\alpha_i = 0$, and $0 \leq \alpha_i \leq c$ for all $1 \leq i \leq n$

Where,

$K(x_j, x_i)$ = Kernel function

α_i =Lagrange multipliers

To satisfy Kuhn-Tucker (KKT), x_i must correspond $0 \leq \alpha_i \leq c$ and $\sum_{i=1}^{n} y_i\,\alpha_i = 0$ and they are called as support vectors.

With the help of equation (2) we can get [1]

$$w = \sum_{i=1}^{n}\alpha_i\,y_i\,x_i \quad (3)$$

Thus the decision function can be represented as

$$f(x, \alpha, b) = \{\pm\} = \text{sign}\left(\sum_{i=1}^{n} y_i\,\alpha_i\,K(x, x_j) + b\right)$$

SVM is more suitable for misbehavior detection than other method. In supervised learning, a

SMS is trained firstly, then this trained machine is used to predict the new data set.

A. Training of SVM classifier

SVM classifier is trained with SVM train function. The syntax used is

$$SVMstruct = \text{svmtrain}(data, groups, 'Kernel\_function', 'rbf')$$

The inputs are,

Data-data is represented as matrix of data points, where row represents one observation and column represents other observation.

Groups-it is the column vector of each corresponding row. Groups must have two types of entries either logical or cell array with two values.

Kernel function- It is used to map the training data set to the kernel space [17].The default kernel function is the dot product. There are several types of kernel function such as linear (meaning dot product), quadratic, polynomial (default value is 3), 'rbf' (Gaussian Radial Basis Function kernel with a default scaling factor, sigma, of 1) kernel function etc.

V. Proposed Work

This section describes a novel support vector machine based trusted dynamic source routing protocol, which uses 'Trust Prediction' concept and is extended from the source routing mechanism Wenjia Li et. al. [10] uses a new concept to categorize the node on their behavior and trust is computed through the Support Vector Machine. In this method trust between nodes is maintained with the help of behavior metrics such as Packet Drop ratio, packet modification ratio and packet misroute ratio. The proposed scheme used instead of packet drop ratio.

A. Proposed SVM based Trust Prediction Method

Support vector machine based method is basically used for detection of malicious nodes and to restrict the data transmission through these nodes. To evaluate performance in the following metrics is used by SVM-Packet Delivery Ratio (PDR), Packet Misroute Ratio (PMIR), Packet Modification Ratio (PMR) and Control overhead CO.

B. Detection of Malicious Nodes using Behavior Metrics

For each specified input SVM receives a set of input data. In this proposed method. SVM collects all the behavior of each node in the network and then compare it with the threshold value T. All of the nodes are classified either trusted or untrusted with the help of the SVM classifier integrating with MANET.

C. Proposed Algorithm

1) Gather all the metrics using NS-3 and save as an XML file.
2) Extract DSR routing transmission and control data (in .XML file) using DOM (Dynamic Object Module) and feed as an input in SVM.
Our proposed work has been checked the route reliability into two phases –

a) Path based on the Behavior of the Node (Relay)
b) Cooperation of the node i.e. Determining Selfishness

These two phases have novelty in our proposed mechanism. The key thing about using these in conjunction is to strengthen the trustworthiness of the route and minimizing the false rate of the prediction of the route before delivery of the packet in MANET using DSR protocol.

a) Path based on the Behavior of the Node (Relay)

3) Calculate PDrp, PDR, PMR, PMIR, Delay, CO
4) Compare the calculated parameter

- if PDR >= .7 then no-operation

  Mark route as "TRUSTED"
- else
  - if (PDR>=0. 5 && PMR <0.65) && ((PMR >= 0.4) && (PMIR > =0. 3)
    Mark route as "UNTRUSTED"
- else
  - if((PDR<0.5&&PMR>=0.6)||PDR<0.5&&PMIR>=5)||PMR<0.7&&PMIR>=0.6)||(PMR>=0.8) ||(PMIR>=0. 7))
    Mark route as "UNTRUSTED"
- else
  Mark route as "TRUSTED"

b) Cooperation of the node i.e. Determining Selfishness
5) For i=0 to n (n= number of nodes present in the MANET topology)

- if (pdr [I] <= 0.5 &&Co [i] >0.25) Then
  node [i] = S (S = Selfish Node)
  then:

goto step [4]

- else node [i] = T (T = Trusted Node)

Mark route as "TRUSTED"

VI. Experimental Setup

A. Metrics for Simulation

In our proposed work, following metric will be used for computing the trust value and then classify the nodes using machine learning approach such as SVM (Support Vector Machine)-

1) PDR (Packet Delivery Ratio)-

$$PDR = (\text{No. of pktsTransmitted}) / (\text{Total no. of Incoming pkts})$$

2) Packet Drop Ratio (PDrp)

$$PDrp = (\text{No. of pkt Drop}) / (\text{Total No. of incoming packets})$$

3) Packet Misroute Rate (PMIR)

The ratio between the numbers of packet misroute to the total no of packet forwarded to the destination.

$$PMIR = \frac{\text{No. of pkts misrouted}}{\text{Total No. of packets forwarded}}$$

4) Packet Modification Ratio (PMR)

It is the proportion of the total number of packet modified to the total number of incoming packets.

$$PMR = \frac{\text{No. of pkts modified}}{\text{Total No. of incoming packets}}$$

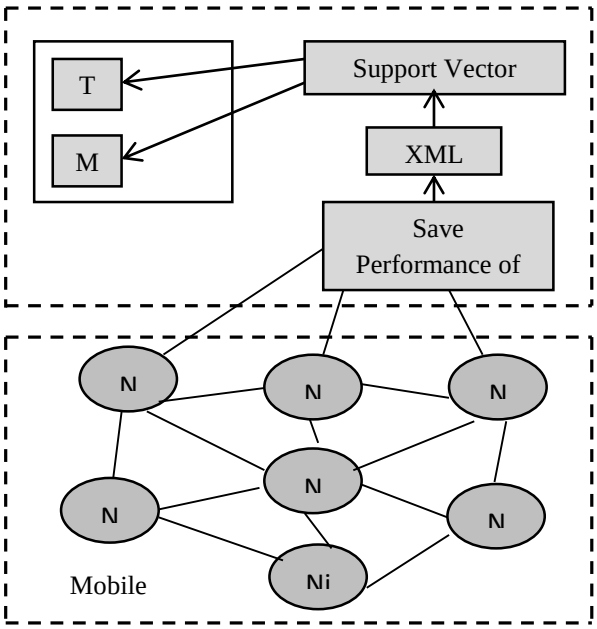
5) Path Optimality (PO)

It is the ratio between the total numbers of Hopes in the shortest path to the one of the Hope in the path taken by a data packet.

6) CO (Control Overhead)

It is a measure of the total number of routing packets sends by a node.

The proposed method is modest and provides fast and rapid response to a suspicious or compromised node. Figure 1 shows the flow of our proposed method.



T: Trusted Node, M: Malicious Node

Fig. 1. SVM based Reorganization System

B. Simulation Parameters and Result Analysis

NS3 simulator version (3.18) is mostly used to evaluate the performance of all the routing protocols in

different conditions [18]. In this simulation experiment, total simulation time is taken 600 Sec. and there are total 30 nodes in the network. Traffic is being carried using UDP datagram, and the size of packet is 512 bytes and random waypoint mobility model is used for simulation.

Table 1. Fixed simulation parameters

Parameter	Value
Simulation time	600s
Number of nodes	30
Map size	1000m*1000m
Mobility model	Random way point
Traffic type	UDP
Transmission radius	250 m
Packet size	512 Bytes
Connections	10
Connection rate	4 pkts/s
Pause time	5 Sec

Figure 2 shows the SVM based classification of trusted and untrusted nodes. A node can be well classified with proposed STDSR because it uses SVM based classification and it classified nodes into two categories: trusted and untrusted node.

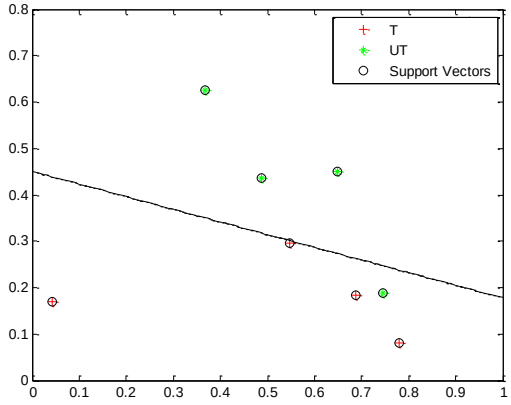


Fig. 2. SVM Based Classification of Nodes

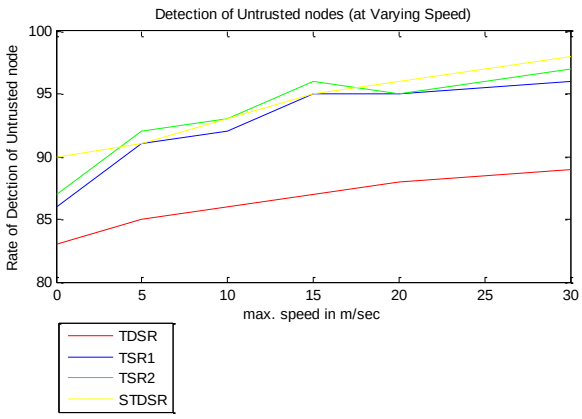


Fig. 3. Graph for Rate of Untrusted node with enhancement of mobility and malicious node

Figure 3 illustrates that the detection ratio of TDSR and TSR increases with node speed. When the interaction among nodes increases gradually, then it is observed that nodes move faster. This leads to a higher detection ratio of malicious nodes. Performance of STDSR is better than TDSR, TSR1 and TSR2 because it uses SVM based classification for detection of malicious nodes.

Table 2. Detection of untrusted nodes versus max. Speed of nodes

Max. Speed in m/Sec	Rate of detection of untrusted node			
	TDSR	TSR1	TSR2	STDSR
0	83	86	87	90
5	83.5	90.05	92	91
10	84	91.35	92	92
15	84.5	91	95	93
20	86	92.21	92	94
25	87	92.5	93	95
30	88	93	94	96

Advantage of STDSR over TDSR when node speed is 0 m/Sec

$$\text{Advantage of STDSR over TDSR} = \frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{90 - 83}{83}\right| * 100 = 8.4337$$

Advantage of STDSR over TDSR when nodes Speed is 5 m/Sec

$$\text{Advantage of STDSR over TDSR} = \frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{91 - 83.5}{83.5}\right| * 100 = 8.952$$

Advantage of STDSR over TDSR when nodes Speed is 10 m/Sec

$$\text{Advantage of STDSR over TDSR} = \frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{92 - 84}{84}\right| * 100 = 9.52$$

Advantage of STDSR over TDSR when nodes Speed is 15 m/Sec

$$\text{Advantage of STDSR over TDSR} = \frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{93 - 84.5}{84.5}\right| * 100 = 10.05$$

Advantage of STDSR over TDSR when nodes Speed is 20 m/Sec

$$\text{Advantage of STDSR over TDSR} = \frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{94 - 86}{86}\right| * 100 = 9.30$$

Advantage of STDSR over TDSR when nodes Speed is 25 m/Sec

$$\text{Advantage of STDSR over TDSR} = \frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{95 - 87}{87}\right| * 100 = 9.19$$

Advantage of STDSR over TDSR when nodes Speed is 30 m/Sec

Advantage of STDSR over TDSR =

$$\frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{96 - 88}{88}\right| * 100 = 9.09$$

In the similar way advantage of STDSR over TDS1 and TSR2 is calculated and the results shown in the table 3.

Table 3. Overall Performance Gain of STDSR with mobility

Max. Speed in m/Sec	Overall Performance Gain of STDSR		
	STDSR Over TDSR	STDSR over TSR1	STDSR over TSR2
0	8.4337	4.651	3.44
5	8.982	1.054	1.086
10	9.52	0.711	0
15	10.05	2.197	2.105
20	9.30	1.941	2.173
25	9.19	2.702	2.150
30	9.09	3.225	2.127

Table 3 shows the overall % gain of support vector machine based trusted dynamic source routing protocol (STDSR) and it is analyzed that STDSR is more suitable for detection of malicious node when compared with the TDSR and TSR protocol.

Figure 4 also shows that the detection ratio of STDSR, TDSR and TSR with varying number of malicious nodes. And result shows that the detection rate of malicious nodes decreasing with the increasing number of malicious nodes. It shows that at high mobility STDSR works well then the TDSR and TSR because it uses the SVM based classification of nodes.

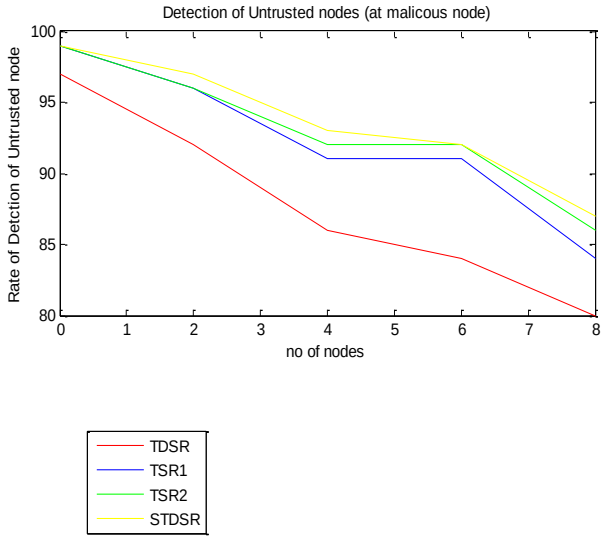


Fig. 4. Graph for Rate of Untrusted node with enhancement of malicious node

Table 4. Detection of untrusted nodes versus no. of malicious nodes

No. of malicious nodes	Rate of detection of untrusted node			
	TDSR	TSR1	TSR2	STDSR
0	97	99	99	99
2	92	96	96	97
4	86	91	92	93
6	84	91	92	92
8	80	84	86	87

Advantage of STDSR over TDSR when no. of malicious node= 0

Advantage of STDSR over TDSR =

$$\frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{99 - 97}{97}\right| * 100 = 2.062$$

Advantage of STDSR over TDSR when no. of malicious node= 2

Advantage of STDSR over TDSR =

$$\frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{97 - 92}{92}\right| * 100 = 5.438$$

Advantage of STDSR over TDSR when no. of malicious nodes= 4

Advantage of STDSR over TDSR =

$$\frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{93 - 86}{86}\right| * 100 = 8.14$$

Advantage of STDSR over TDSR when no. of malicious nodes= 6

Advantage of STDSR over TDSR =

$$\frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{92 - 84}{84}\right| * 100 = 9.524$$

Advantage of STDSR over TDSR when no. of malicious nodes= 4

Advantage of STDSR over TDSR =

$$\frac{\text{STDSR} - \text{TDSR}}{\text{TDSR}} * 100 = \left|\frac{87 - 80}{80}\right| * 100 = 8.75$$

In the similar way advantage of STDSR over TDS1 and TSR2 is calculated and the results shown in the table 5.

Table 5. Overall Performance Gain of STDSR with no. of malicious nodes

No. of Malicious Nodes	Overall Performance Gain of STDSR		
	STDSR Over TDSR	STDSR over TSR1	STDSR over TSR2
0	2.062	0	0
2	5.438	1.042	1.042
4	8.14	2.198	1.087
6	9.524	1.098	0
8	8.75	3.571	1.163

Table 5 shows the overall % gain of support vector machine based trusted dynamic source routing protocol (STDSR) and it is analyzed that STDSR is more relevant for detection of malicious node when related with the TDSR and TSR protocol.

VII. Conclusion

This paper introduced support vector machine based DSR protocol for safeguarding routing in mobile ad-hoc network and it is examining that performance of STDSR increases in some performance indicator such as detection ratio with the variation of mobility and number of malicious nodes, and in future this proposed protocol can be used to show that the performance of STDSR increases in some other parameter such as a packet delivery ratio, average end to end delay, and throughput.

VIII. Future Work

In future this proposed protocol can also be used in Wi MAX and vehicular ad-hoc network.in future we also evaluate the performance of STDSR with other parameters such as a packet delivery ratio, average end to end delay, and throughput.

References

[1] CHENG Yong, HUANG Chuanhe, SHI Wenming: Trusted Dynamic Source Routing Protocol: Published by the IEEE Computer Society 2007, 1623-1636.

[2] H. Xia1 Z. Jia1 L. Ju1 Y. Zhu2: Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory: Published in IET Wireless Sensor Systems, Vol. 1, Iss. 4, pp. 248–266.

[3] DilpreetKaur and Naresh Kumar: Comparative Analysis of AODV, OLSR, TORA, DSR and DSDV Routing Protocols in Mobile Ad-Hoc Networks: Published Online March 2013 in MECS, pp.39-46.

[4] Zhaoyu Liu, AnthonyW. Joy, Robert A. Thompson: A Dynamic Trust Model for Mobile Ad Hoc Networks: Proceedings of the 10th IEEE International Workshop on Future Trends of Distributed Computing Systems (FTDCS'04) IEEE 2004

[5] ELIZABETHM and ROYER, CHAI-KEONG TOH: A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks: published in IEEE Personal Communications 1999, pp.46-55

[6] Mohammad Wazid, Rajesh Kumar Singh: A Survey of Attacks Happened at Different Layers of Mobile Ad-Hoc Network & Some Available Detection Techniques: Proceedings published by International Journal of Computer Applications (IJCA) International Conference on Computer Communication and Networks CSI-COMNET-2011, pp.44-49.

[7] N. Bhalaji, A. R. Sivaramkrishnan, Sinchan Banerjee, V. Sundar, and A. Shanmugam: Trust Enhanced Dynamic Source Routing ProtocolforAdhoc Network: World Academy of Science, Engineering and Technology 49 2009, pp- 1074-1079

[8] Asad Amir Pirzada, Chris McDonald, and AmitavaDatta: Performance Comparison of Trust-Based Reactive Routing Protocols: published in IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 5, NO. 6, JUNE 2006, pp. 695-710

[9] Hui Xia a, ZhipingJia, Lei Ju, Xin Li, Edwin H.-M.Sha: Impact of trust model on on-demand multi-path routing in mobile ad hoc networks: published in science direct 2013, pp.1078–1093

[10] Wenjia Li, Anupam Joshi, Tim Finin: SAT: an SVM-based Automated Trust Management System for Mobile Ad-hoc Networks: 2009.

[11] S. Marti, T.J. Giuli, K. Lai, M. Baker: Mitigating routing misbehavior in mobile ad-hoc networks: Mobile Computing and Networking (2000) 255–265

[12] YIH-CHUN HU∗ and ADRIAN PERRIG: Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks: published springer 2005, pp. 21–38

[13] Sergio Pastrana, AikateriniMitrokotsa, Agustin Orfila, Pedro Peris-Lopez: Evaluation of classification algorithms for intrusion detection in MANETs: published in science direct 2012,pp-217–225

[14] Hui Xia, Zhipingjia, Xin Li, Lei ju: Trust Prediction and Trust-based source routing in mobile ad hoc networks: Computer Communications 2012, pp- 2096–2114

[15] S. Rajasegarar, C. Leckie, and M. Palaniswami: Detecting Data Anomalies in Wireless Sensor Networks: Security in Ad hoc and Sensor Network, Computer and Network Security , World Scientific Publishing Co, Vol. 3, pp.231-259, 2009.

[16] Meenakshi Patel, Sanjay Sharma: Detection of Malicious Attack in MANETA Behavioral Approach: published in 3rd IEEE International Advance Computing Conference (IACC), 2012, pp-388-392

[17] B. Scholkopf, and A. J. Smola: Learning with Kernels: The MIT Press, 2006, pp.204-205.

[18] NS-3 Network Simulator. http://www.nsnam.org, July 2009.

Authors' Profile

Priya Kautoo: received his Bachelor`s degree in Computer Science and Engineering, GGCT, Jabalpur, India in 2010.At present she is pursuing her M.E. degree in Computer Science & Engineering from UIT-RGPV, Bhopal India. Her research areas are Computer Networks, Security in Ad-Hoc Network.

Dr. Piyush Kumar Shukla: received his Bachelor's degree in Electronics & Communication Engineering, LNCT, Bhopal in 2001, M. Tech (Computer Science & Engineering) in 2005 from SATI, Vidisha and Ph.D. (Computer Science & Engineering) in 2013 from RGPV, Bhopal. M.P. India. He is a member of IEEE, IACSIT. Currently he is working as an Assistant Prof. in Department of Computer Science & Engineering, UIT-RGPV Bhopal. He is also I/C of PG Courses in DoCSE, UIT, RGPV. He has published more than 40 Research Papers in various International & National Journals & Conferences.

Dr. Sanjay Silakari: received his Bachelor's degree in Computer Science & Engineering from SATI, Vidisha in 1991,

M.E. (Computer Science & Engineering) from DAVV, Indore in 1998) and Ph.D. (Computer Science & Engineering) in 2006 from B.U. Bhopal (M.P.) India. He has published more than hundreds Research Papers in various International & National Journals & Conferences. He is Dean of Faculty of CSE & IT in RGPV. Currently He is working as Joint Director in UIT-RGPV and Prof. & Head in CSE Department, UIT-RGPV Bhopal. He is also member of various Academic Societies.He has several research publications to his credit in different reputed national and international conferences & journals. He has edited the proceeding of different international conferences including IEEE conference, & also organized & attended several international & national conferences. He is a life member of India Society for Technical Education (ISTE), Computer Society of India (CSI), the Indian Science Congress Association & International Association of Engineers (IAENG), & a member of IEEE and ACM.

How to cite this paper: Priya Kautoo, Piyush Kumar Shukla, Sanjay Silakari,"Trust Formulization in Dynamic Source Routing Protocol Using SVM", International Journal of Information Technology and Computer Science(IJITCS), vol.6, no.8, pp.43-50, 2014. DOI: 10.5815/ijitcs.2014.08.06

