International Journal of Information Retrieval Research
Volume 12 • Issue 3

Integration of Multi-Class Service Paradigm With Generic Trust Mechanism for Innovation, Customization and Adaptability in MANETs

Nitin Khanna, Kanya Maha Vidyalaya Jalandhar, India*
Sandeep Singh, CT University, India
Anshu Bhasin, I. K. G. Punjab Technical University, India
Kamal Malik, CT University, India

ABSTRACT

Trust-based mechanisms are widely used in wireless networks of different kinds for providing security against attack. Trust mechanism provides security from various attacks using both detective and preventive manner. This paper presents a quality service paradigm that can be integrated with any underlying trust mechanism. The paradigm includes different flags corresponding to different services incorporated in various routing packets. The paradigm provides flexible customization and adaptability as per the demand of communicating nodes for effective data transfer. Various quality service classes are designed to formulate route as per the requirement to minimize the routing overhead and balancing of load among nodes. This paradigm power is the trust mechanism with proactive action for detection of malicious nodes in the network. The proposed paradigm is incorporated in an established trust mechanism and compared with standard version of that trust mechanism for packet delivery ratio and routing overhead.

KEYWORDS

Fictitious Node, Link Stability Index, Quality Service Class, Routing Protocol, Trust Mechanism, Trust Value, Wireless Networks

1. INTRODUCTION

With the invention of new technologies, the adaptation of wireless ad-hoc networks has increased to large extent (Zhang et al., 2012), (Moussaoui et al, 2014). The ad-hoc networks have many important applications like WSN, IOT, MANET, VANET and FANET in different fields that attracts the researchers (Triparty et al., 2020), (Jiang et al., 2020), (Chen et al., 2020). Nodes or devices in these types of networks are capable of self-configuration without any centralized control to operate in the network (Mayti et al., 2017). Some networks involve movement of nodes making the network topology

DOI: 10.4018/IJIRR.300290 *Corresponding Author

highly dynamic (Khan et al., 2017). The communication among nodes in such networks is achieved in multi hop manner. Intermediate nodes are used to set up a route between sender and receiver (Wei et al., 2014). However, these intermediates nodes may be malicious and can attack the network in many different ways in order to hamper communication in the network. Hence, the ad-hoc networks have more security issues than their counterparts.

Various mechanisms like routing based (Gupta et al., 2019), trust based (Huang et al., 2020), cluster based (Subba et al., 2015), sequence number based (Rajesh Babu & Usha, 2016), overhearing based (Kollati & Somasundaram, (2017), cross-layer based (Usha et al.,2017), cryptography and authentication, etc. are used by researchers to enhance the security of wireless ad-hoc networks. Out of all security mechanisms, trust based mechanisms have attracted the researchers more due to their preventive nature, effectiveness, accuracy and scalability. Trust based systems can deal with simple as well as smart or intelligent attacks like co-operative blackhole (Singh et al., (2021) and grayhole attacks (Khanna & Sachdeva, 2019). One more advantage of trust based frameworks is that they can work in collaboration with other mechanisms and integrate seamlessly with base routing protocols to provide all-inclusive security in smart networks (Alnumay et al., 2019).

Trust based mechanisms support both prevention and detection of malicious nodes in a network (Hammamouche et al., 2018), (Zhang et al., 2019). Prevention is achieved through forming routes that are more trustworthy. For detection, trust based mechanisms periodically update the trust value of all the active nodes to detect the malicious nodes. In trust based system, we can continuously observe the performance and behavioural patterns of neighbouring nodes in the network (Bhasin et al., 2020). If any malicious node is found during this periodic check, that node(s) is marked malicious and information related to it is broadcasted in the network and as a result that node becomes isolated in the network. Trust based frameworks enhances the overall performance of network in terms Quality of Service, robustness, packet delivery ratio, and throughput.

Trust can be calculated in variety of ways. It can be direct, indirect or historical. It incorporates various network parameters for calculations.The major components in most trust based systems are real time information collection, trust evaluation, decision making and dissemination unit (Khanna & Sachdeva, 2019). Real time information collection component gathers required information related to communication behaviour of active nodes. Trust evaluation component uses the information gathered by the information collection component to calculate the trust. Decision making component is responsible for filtering the malicious and genuine nodes after considering the final trust of all nodes. The nodes having low trust value than the defined threshold value are declared as malicious nodes. Dissemination unit broadcasts the identity of malicious node in the network so that the detected malicious node can be isolated. Various trust frameworks have been developed so far by the different researchers in this field, but most of the frameworks suffers from high routing overhead, high energy consumption and high false positive rate. This decreases the overall throughput of the network.

The main idea of this paper is to propose a Multi-Class Service Paradigm which provides differentiation of service classes that can be used to make routes as per the requirements. This customization can help in proactive detection of attacking nodes and forming adaptable routes as per requirement which significantly decrease the routing overhead.

Major contributions of this research are presented as follow:

1. Framing of Multi-Class Service Paradigm that can be applied to any generic trust mechanism and base routing protocol.
2. Multi-Service classes provide flexibility in formation of routes as per the requirements.
3. A balanced approach in trust mechanisms that provides proactive detection as well as prevention from attacking nodes.
4. Application of Link Stability Index for identification of link strength.

In section II, a brief review of trust based mechanisms which deals with various routing attacks is presented. In Section III, the methodology of Multi-Class Service Paradigm is presented, that includes the modifications in the routing packets of base protocol. This also includes brief introduction of various flags applied for defining classes. After that, multi-service classes along with their application for customization in various scenarios is presented. Section IV presents the simulation environment under which the proposed paradigm is integrated with trust mechanism and validated. Section V includes results and discussions to highlight the impact of multi service class approach. In the final section, the conclusion along with scope of further research work on the subject is discussed.

2. BACKGROUND

(Wadhwani et al., 2020) presented a method in which trust of each node is calculated by counting number of RREQ and RREP packets sent to nearby nodes. (Josephine et al., 2020) suggested a mechanism in which each node is evaluated on the basis three factors. Authors used support vector regression method initially to create weak learner, and ensemble classifier afterwards to create strong classification. (Merlin et al., 2019) proposed an approach which uses direct and indirect trusts to find the comprehensive trust. Dynamic generation of multiple detection routes is done to mitigate the malicious nodes.(Manoranjini et al., 2019) introduced a method which uses trust metrics such as social trust, service trust and QoS trust to detect malicious nodes. (Shanthi et al., 2018) adopted a cluster based mechanism in which trust value of cluster members and other cluster heads is maintained by each cluster head. Final trust is calculated on the basis of forwarding nature and recommendation from other cluster heads. If the trust of a node falls below a threshold value, that node is declared as malicious. Group key management process is used for secure and confidential communication. (Beghriche & Bilami et al., 2018) used a fuzzy based trust mechanism to find the optimal path with little to no chance for attacking node. They used the grey relational analysis along with fuzzy model to compute the trust of nodes based on observations. However, implementation of this protocol is not independent and lacks adaptability to the dynamic needs of the network. (Salman et al., 2018) suggested a trust-based routing mechanism TSQRS in which they merged social and QoS parameters to calculate the trust. To exchange the trust values of nodes, Hello Messages are modified. QoS parameters offers more adaptability and efficient use of resources with improved security. In ESCT mechanism (Cai et al., 2018) nodes co-operate with each other to detect the smart attacks by exchanging various records. Trust is calculated on the basis of packet forwarding ratio only and each node make judgment regarding the malicious node on the basis of their own cognitive judgment. They also used voting system in cooperative detection so that malicious nodes cannot increase their trust mutually. TRAB-IDS (Anusha & Sathiyamoorthy, 2017) mechanism employs trust framework over IDS. They used the concept of certificate authority to make the mechanism robust. The certificate authority is responsible for generating the public and private key to authenticate the neighboring nodes. The use of trust and cryptography makes the intrusion detection procedure more accurate and decreases the false positive. However, it suffers from high computational overhead and high energy consumption. (Zhao et al., 2016) introduced a mechanism DATEA which uses direct trust, communication trust, indirect trust, and historical trust. The adaptive weighting method is used to assign weights to all trust components. This mechanism provides accurate trust calculation and hence effectively prevents most of the blackhole attacks. ReTEAODV (Sethuraman & Kannan, 2016) a trust based mechanism which uses both direct and indirect trust to compute the final trust. Bayesian probability is also used for finding the refined trust. The proposed method selects the route which uses less energy and is trustful for communicating the packets. (Xia et al., 2015) suggested a light weight trust-based routing approach TeAOMDV in which trust is calculated using multidimensional trust parameters. The weights of the direct trust parameters are calculated using fuzzy model based on entropy weight measure. For quick calculation of trust, a matrix has been defined at each node. It is basically a prevention approach that provides reliable paths with high trust values. (Biswas & Nag, 2014) adopted a trust

based system to discover both blackhole and cooperative blackhole attacks with efficient utilization of resources. Three parameters named as Rank, Remaining Battery Power, and Stability factor are used to calculate the trust of a node in the network. Due to the assumptions, it suffers from false positive. (Subramaniyan et al., 2014) presented a mechanism RTBD to efficiently detect the malicious nodes. Each node has to maintain a trust table. The trust value of a node is updated when there is new trust certificate. This new trust value is also verified from neighbors. Based on the trust value a node, it can be declared as malicious or legitimate node. Once the node is declared as malicious, its identity is shared in the network. (Mohanpriya & Krishnamurthy, 2014) suggested a method TBDSR, in which each node replies to RREQ packet in the form of RREP packet which contains the trust value of its next hop node. If the reply is from destination node, then the data is sent to destination node. But if the reply is from an intermediate node its trust value is verified from other nodes using BHREQ and BHREP packets introduced in this method.

The trust based mechanism provides two dimensional security both in terms of prevention and detection against routing attacks in MANET. However, almost every trust mechanism lacks in flexibility and proactive detection approach. This leads to following challenges in present research, which are focused in this paper:

- Trust based mechanisms do not enter into detection phase in proactive manner. The detection phase is always reactive in nature.
- Published trust based mechanism lacks flexibility in forming routes of varying quality as per the demand of communicating parties.

The above identified aspects are considered to motivate our approach for immaculate customization and enhanced adaptability in MANET.

3. METHODOLOGY

In this section, the Multi-Class Service Paradigm (MCSP) is defined which requires enhancements in base routing protocol to incorporate various fields and flags. Seven service classes are designed to formulate route as per the requirements to minimize the routing overhead and load balancing among nodes. This paradigm includes different flags corresponding to different services incorporated in various routing packets. Customization and adaptability as per the requirement of communicating nodes is ensured to formulate routes that serve different purposes along with proactive detection of nodes that are involved in packet drop attacks.

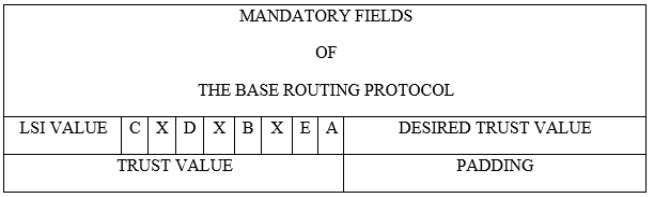
3.1 Enhancements in Routing Protocol

The routing protocol defines the set of standards that are followed for route establishment and its maintenance. In this research, a generic routing protocol is employed which signifies that the MCSP mechanism works fine with all categories of routing protocols whether it be pro-active, re-active or hybrid. Enhancement in routing protocol is performed by incorporating different fields and by introducing new packets in the standard protocol to serve different purposes.

3.1.1 Route Request PACKET

The format of route request packet in the routing protocol is presented in figure 1. This packet apart from the general and mandatory fields of a routing protocol includes the trust notion. The general fields in the route request packet includes type, unique identifier, IP addresses, sequence number of the packet, hop count and various other options. A set of flags are included in this packet that defines the service class of data communication. The service class represents the services which are

Figure 1. Fields of Route Request Packet



to be provided by the route formed through the reply packet. These flags are used to identify the requirements of the source node from a particular route which it wants to be formed.

The LSI VALUE field represents the minimum Link Stability Index value associated with the path which is so far covered by this request packet. The TRUST VALUE field represents the trust value associated with the path covered by this packet as well. The DESIRED TRUST VALUE becomes significant when a particular flag is set and includes the minimum trust value desired by the source node. The details of fields of route request packet are given in table 1.

The details of various flags are provided during the differentiation of service classes in section 3.2. More than one flag can be set and they are to be in conjunction, if possible. In case, the flags are contradictory in nature and are set simultaneously, then flag closest to LSI VALUE field holds precedence and will be effective.

3.1.2 Route Reply Packet

The packet format for route reply is presented in figure 2. It also incorporates trust notion, IP address of the generator, service flags and Link Stability Index of the route proposed. The route reply packet is generated when the intermediate hop has the route to the designated destination. The designated destination is found from route request packet in response to which route reply packet is generated. The IP address of the intermediate node or the destination that generates the route reply packet is placed in the Generator IP Address field.

The details of fields of Route Reply packet are given in the table 2.

Rest of the fields have same description for reply packet as that of route request packet.

Table 1. Details of Fields of Route Request Packet

Field Name	Description
TRUST VALUE	Trust value of the path so far. The floating point trust value between 0 to 1 is mapped to 16-bit binary number.
DESIRED TRUST VALUE	Minimum trust value required for the route to be established. This field will be significant only if D flag is set.
LSI VALUE	Average Link Stability Index value of the path so far. Ignored if B flag is not set.
A Flag	Acknowledgement Flag.
B Flag	Burst Data Flag.
C Flag	Critical Data Flag.
D Flag	Desired Flag.
E Flag	Exclusive Flag.
X	Don’t Care.

Figure 2. Format of Route Reply Packet

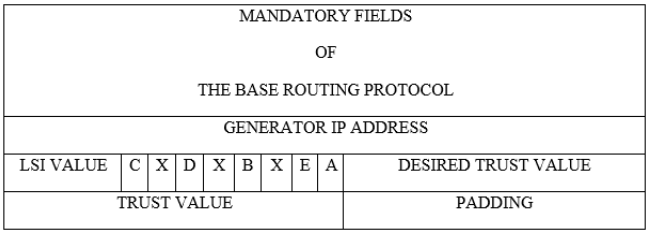


Table 2. Details of Fields of Enhanced Route Reply packet

Field Name	Description
TRUST VALUE	Trust value of the route for which the reply message is generated and directed towards the source node.
LSI VALUE	Average Link Stability Index value of the path formed. Ignored if B flag is not set.

3.1.3 Data Packet

Format of data packet in the generic routing protocol is presented in figure 3. The data packet has only one additional field in the standard format to include the trust notion.

3.1.4 Ping Message

This packet is used by each node to share information with its neighbouring nodes. The format of this packet is represented in figure 4. It shares information like list of malicious nodes that are marked by this node as malicious. Residual battery level is also shared by the node for itself. Checksum and Header Length (HLEN) is used to provide error detection and length of header of this packet.

Figure 3. Format of Data packet

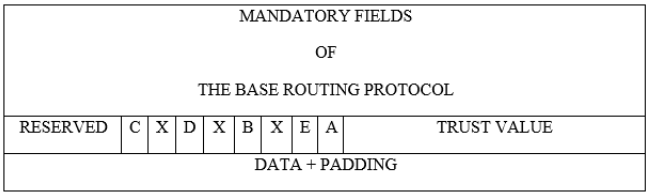
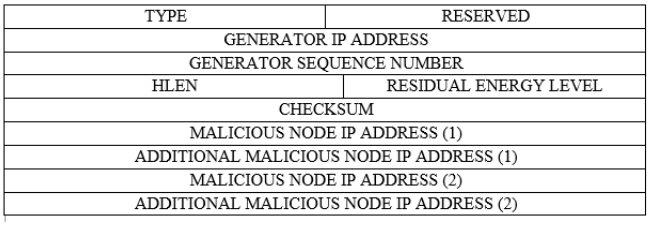


Figure 4. Format of PING packet



The details of fields along with their size in bits are given in the table 3.

Equation 1 represents the overhead ratio which is defined as the ratio of overhead caused by the routing protocol in standard form and MCSP mechanism. This formulates the relation between the routing protocol and proposed mechanism MCSP in terms of overhead. As this ratio falls below 1, it indicates that the MCSP mechanism works well in bringing the routing overhead down. This equation is used in simulation to define results related to routing overhead.

$$Overhead\ Ratio = \frac{n_1 \times RREQ_i + n_2 \times RREP_i + n_3 \times DATA_i + n_4 \times PING_i}{m_1 \times (RREQ_i + 64) + m_2 \times \left(RREP_i + 64\right) + m_3 \times \left(DATA_i + 32\right) + m_4 \times (PING_i + \left[\frac{T}{2}\right] \times 32)} \quad (1)$$

3.2 Multi-Class Service Paradigm

The Multi-Class Service Paradigm is divided into seven classes according to the value set of different flags. Depending upon the combination of flags set, the route, which is being requested by the source node is categorized. Table 4 includes description of Flags applied in Multi-Class Service Paradigm.

The service classes associated with different combinations of flags mentioned in table 4 are described as follows in detail.

Table 3. Fields of PING packet

Field Name	Size (in bits)	Description
GENERATOR IP ADDRESS	32	The IP address of the generator of this packet.
GENERATOR SEQUENCE NUMBER	32	Sequence number of the generator node.
RESIDUAL ENERGY LEVEL	16	Residual battery of the generator node.
HLEN	16	Length of the Header in BYTES.
MALICIOUS NODE IP ADDRESS (1)	Variable (Multiple of 32 bits)	List of IP addresses of nodes that are marked as attacking nodes and given second chance.
MALICIOUS NODE IP ADDRESS (2)	Variable (Multiple of 32 bits)	List of IP addresses of nodes that are marked as attacking nodes have exhausted their second chance.

Table 4. Description of Flags applied in Multi-Class Service Paradigm

Field Name	Description
A Flag	Acknowledgement Flag. This flag is set in case the source node wants Acknowledgement from destination for each data packet received.
B Flag	Burst Data Flag. This is to be set in case a stable connection is required. Link Stability Index plays an important role here and LSI VALUE field becomes significant.
C Flag	Critical Data Flag. It is used in case of critical data transfer which must be received by the destination. In this case the route reply message must be sent by the destination node.
D Flag	Desired Flag. It provides flexibility in choosing the trust value of the path as desired by the source node. DESIRED TRUST VALUE FIELD have significance only if D flag is set.
E Flag	Exclusive Flag. It is used by the source node that needs to send few data packet to a particular node and requires a short communication.

3.2.1 Default Class

This is a set of service classes in which only a single flag is set to 1, while all the remaining flags are set to 0. This set of classes is utilized to see the default behaviour of different flags. This set of classes is utilized to avail the benefit of individual flags. For instance, flag A is set to ensure that the destination node correctly receives data sent by the source. This is achieved through Acknowledgment packet sent by destination to the source on receiving data packet correctly.

All the flags are independent of each other and are non-contradictory except the flag B and flag E. The flag B refers to the burst transfer involving exchange of high number of data packets, while flag E refers to lower number of data packet exchange. These two flags are contradictory to each other and setting both the flags does not make sense. So, flag B is given priority over flag E, i.e., if both the flags are set, then flag B will be effective while flag E is ignored.

3.2.2 Fictitious Path Class

This class can be used to identify a malicious node in a proactive manner. This class needs flag A and flag E to be set. The rest of the flags can have any value while flag B is set to 0. The source node proactively asks for a route to a fake destination which does not exist. If any node claims to have a path to the fake destination will ultimately marked as malicious. As that node cannot have the path to a non-existing node, it proves that the node generates a fake Route Reply and hence is marked as malicious.

3.2.3 Reliable Burst Class

This service class is used to form a reliable path that has a relatively better stability. For this service class, the flag A and B must be set to 1, while other flags can either be set to 0 or 1. This class is used when there is a need for a stable and reliable path for bulk data transfer over a period of time. When a node needs to send a burst of data packets to a particular destination, it asks for the stable route by setting A and B flags in the Route Request packet. Flag A is set to ensure that the destination will send acknowledgement for each data packet received. Flag B enables LSI field that is used to evaluate the stability of the route. The route selected will have a higher LSI value.

Thus, the route formed will survive for the entire burst duration and the entire data is reliably communicated to the destination. LSI value for a pair of neighbouring nodes increases by 1 for each unit time and is reset to zero in case the link is broken with the neighbouring node. In this way, LSI acts as an indicator of strength of link between two neighbours. A higher LSI value means a strong and stable connection among them in both directions.

3.2.4 Critical Communication Class

This service class is used to establish a route that is most genuine. The data that is to be communicated through the path must be delivered to the destination and no compromise in path formation is made. So, the route reply packet must come from the destination itself and each data packet must be acknowledged. For this class, A and C flag must be set to 1, while the other flags can have any of the values. When this class is utilized, the Route Reply generated by intermediate nodes are ignored.

3.2.5 Short Communication Class

This service class is used in case a source needs to send only one or a few data packets to a particular destination and the requirement of receipt of data packet by the destination is not critical. For this class E flag must be set to 1 while A, B and C flags must be set to 0. All the remaining flags can have either value. Generally non-critical data is communicated through this class. The shortest or quickest path is selected in this case.

3.2.6 Fixed Minimum Trust Class

This service class is utilized to establish a route that has a trust value of desired level. For this class, D flag must be set to 1, while all the remaining flags can have any value. This class provides different level of quality to the data communication as different paths to a particular destination can be formed as per the trust requirement. If there is need of reliable communication, trust value of prospective path has to be high. When a node asks for a route having a particular level of trust at least, then it will ignore any Route Reply with trust value lower than the desired trust value. For each received Route Reply, the trust in the trust value field and desired trust value field are compared.

3.2.7 Hybrid Class

Hybrid service class is a combination of two or more aforementioned classes. For instance, if a critical reliable burst data transfer is needed, then flags are set to the values that reflects the attributes of both critical communication and reliable burst quality service classes. For this purpose, both A, B and C flag must be set to 1 while the remaining flags can assume any value.

3.3 Generalization of Trust Paradigm

The trust paradigm established in this paper can be generalised through a triple layer approach. The bottom layer deals with the routing aspect in which an underlying routing protocol is used. This routing protocol is enhanced to incorporate notion of trust as well as the proposed multi-class service paradigm. In middle layer, the effective characteristics of trust based mechanism are exploited for mitigation of attacking nodes. The topmost layer is the actual proposed multi-class service paradigm that is built over the second layer to ensure adaptability and enhancement of effectiveness of underlying routing and mitigation of attacks through trust mechanism.

4. SIMULATION

The simulation of the proposed paradigm is performed through Java-Matlab Interface. Simulation of different scenarios are performed for validation of effectiveness and efficiency of the proposed paradigm on the basis of different parameters. Table 5 includes various simulation parameters fixed for different network scenarios along with their values.

The parameters defined in table 5 are standard simulation parameters for MANETs. Here pause time represents the interval after which the monitored values are analysed and calculations

Table 5. Simulation parameters and their corresponding values

Parameter	Value	Parameter	Value
Number of Nodes	20 40, 60, 80	Confidence Interval	95%
Mobility	0 – 20 metre/sec	Link Type	Asymmetrical Bi-directional
Simulation Area	2000m X 2000m	% of Malicious Node	0 - 50%
Transmission Range	250 metre	Battery Capacity	4000 mAh
Routing Protocol	Enhanced AODV	Mobility Model	Random Waypoint Model
Pause Time	20 seconds	MAC Protocol	802.11a
Antenna Type	Omni-Directional	Data Packet Size	1024 Bytes
Traffic Model	CBR	Types of Attack	Blackhole, Grayhole

are performed for trust update. The mobility model used in simulation is random way point. In this model a particular node selects a random destination point to which it will reach. The node can take any random direction to reach that point in a defined interval of time.

Following assumptions are made to perform simulation:

- The Multi-Class Service Paradigm can be incorporated in any standard trust mechanism without any contradiction.
- During the trust and Link Stability Index update, no communication is performed by the nodes.

The BEST mechanism (Khanna & Sachdeva, 2020) is chosen as benchmark and underlying trust mechanism for simulation and discussion on obtained result. The samples of the results are collected on pause time interval during which trust and LSI values are updated. Scenarios related to all the defined classes are simulated for validation purposes. Trust value, LSI and various flags in control packets are utilised to provide the required services. Default class is validated through 5 scenarios in which a single flag is set to 1 in each of those scenarios. This is done to check the working when only one flag is set. For fictitious path class, a scenario is created in which node N broadcast RREQ packet in the network to find the path for a non-existing node X. This is done in order to find malicious nodes performing packet drop attacks.

For validating reliable burst class, a scenario is created in which node A sends 256 MB data to node B in the form of burst. It is checked through these scenarios that whether the link remains stable throughout the burst or not and if the link breaks how often it happen. In order to validate critical communication class, node A sends RREQ packet to get path for destination D. Node A must check whether RREP packet is generated by node D. Short communication class is validated through a scenario in which node A sends RREQ packet for getting the path to node D and send the packet to the path made from very first route reply packet received. To validate fixed minimum trust class, source node verifies the trust value in the received RREP packet that are generated in response to RREQ packets to find the desired path. The source node accepts only those RREP packet which has trust value higher than the desired trust value.

5. RESULTS AND DISCUSSION

The Multi service class paradigm (MCSP) presented can be incorporated in any type of trust mechanism. The modification in the base routing paradigm is performed to incorporate all flags involved in multi service classes. The proposed MCSP is compared with the BEST mechanism (Khanna & Sachdeva, 2020) on the basis of Packet Delivery Ratio and Routing Overhead. The varying parameter in all the cases is percentage of malicious nodes and their percentage varies from 0-50%. For simplification, the values are averaged out for different simulation scenarios at a certain level of comparison.

5.1. Packet Delivery Ratio

Packet Delivery Ratio is the ratio of number of data packets that are correctly received at the destination nodes to the total number of data packets generated by the source nodes. As shown in equation 2, Packet Delivery Ratio is calculated as the ratio of total number of data packets correctly reached at the destination to total number of data packets sent from source:

$$Packet\,Delivery\,Ratio = \frac{Data\,packets\,correctly\,reached\,destination}{Data\,packets\,sent\,by\,source} \tag{2}$$

It is evident in the figure 5 that PDR is improved significantly in case of MCSP as compared to standard BEST mechanism. This is due to two main reasons. First is the use of fictitious route class which helps the source node to identify the malicious nodes proactively that ultimately decreases the packet drop count. Secondly, the use of reliable burst class along with LSI value lead to formation of stable paths in case of long duration data transfers. This is not the case in the standard mechanism as it does not have the facility of forming routes that are highly stable. For critical transmission, critical communication class ensures the delivery of all the packets due to most reliable path. This is due to the fact RREP packet comes from the destination node itself.

5.2. Routing Overhead

Routing overhead includes the amount of control information sent per unit data information. As shown in equation 3, it is calculated as the amount of control information sent in the form of control packets and route maintenance for sending one unit of data information. The routing overhead generally includes the entire set of control packets and headers of data packets. These do not convey enough actual useful data for the end nodes. For more effective and accurate comparison, calculation is done using the byte as unit for both data and control information instead of the packets:

$$Routing\,Overhead = \frac{Control\,Information\left(in\,Bytes\right)}{Data\,Information\left(in\,Bytes\right)} \tag{3}$$

It is evident in figure 6 that routing overhead in case of MCSP is significantly less as compared to standard BEST mechanism. This is despite of the fact that additional fields and flags are incorporated in data packet and control packet headers. The overhead is still low due to selective flooding of control packets which depends upon type of flags set in the control packets. For instance, in case of Fixed Minimum Trust Class, if the node comes to conclude that now the trust of the path so far formed is falling below the minimum trust requirement, then it will not forward control packets related to that path any further in the network. Also, formation of more stable paths and proactive detection of attacking nodes lead to lesser route errors and hence lesser control information flow as well. However, in case of BEST mechanism, lack of class paradigm does not give it flexibility for selective flooding and

Figure 5. Comparison of Packet Delivery Ratio

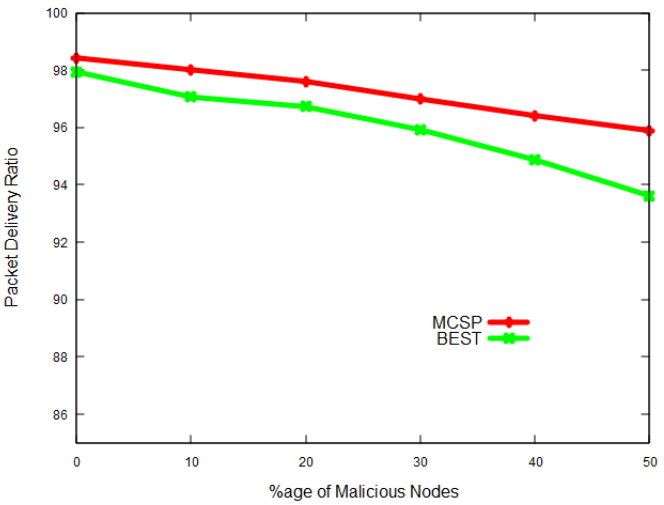
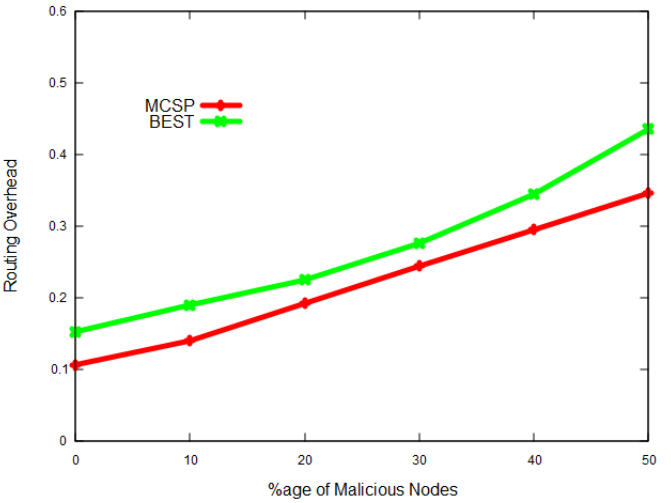


Figure 6. Comparison of Routing Overhead



formation of routes with desired trust value. This ultimately triggers significant increase in routing overhead in case of BEST mechanism in standard form.

6. CONCLUSION

In this paper, a Multi-Class Service Paradigm is presented that integrates with the base routing protocol and underlying trust mechanism. This paradigm strengthens the base trust mechanism by integrating the proactive attack detection facility in it. This is due to the fictitious path class in the paradigm. It also provides the customization and flexibility for route formation as communicating end nodes can form routes as per requirements. The paradigm is included in the generic base routing protocol through five flags A, B, C, D and E each of 1 bit size along with Link Stability Index. This paradigm includes seven classes, i.e., default value, fictitious path, reliable burst, critical communication, short communication, fixed minimum trust and hybrid class. Default value class provides services related to the associated flag. Fictitious path class provides the facility to proactively detect malicious nodes. Reliable burst class facilitates to form stable paths. Critical communication class ensures the formation of most robust path as RREP is generated from the destination itself. Short communication class provides facility for quick and brief communication involving a few data packets. Fixed minimum trust class provides route with the trust value equal or greater than the desired trust value. Hybrid class helps in obtaining the services of two or more classes together. The paradigm is highly scalable and provides the ease of integration with any trust mechanism and routing protocol. The incorporation of paradigm leads to improved packet delivery ratio with a significant decrease in the routing overhead.

The future research activities need to target on scaling the paradigm by incorporating more general as well as specific flags and classes to make the trust mechanism more robust while keeping the routing overhead constant.

FUNDING AGENCY

Publisher has waived the Open Access publishing fee.

REFERENCES

Alnumay, W., Ghosh, U., & Chatterjee, P. (2019). A Trust-Based Predictive Model for Mobile Ad Hoc Network in Internet of Things. *Sensors (Basel)*, *19*(6), 1467. doi:10.3390/s19061467 PMID:30917499

Anusha, K. & Sathiyamoorthy, E. (2017). A new trust-based mechanism for detecting intrusions in MANET. *Information Security Journal: A Global Perspective, 26*(4), 153-165. .10.1080/19393555.2017.1328544

Beghriche, A., & Bilami, A. (2017). A fuzzy trust-based routing model for mitigating the misbehaving nodes in mobile ad hoc networks. International Journal of Intelligent Computing and Cybernetics. doi:10.1108/IJICC-04-2017-0038

Bhasin, A., Singh, S., & Kalia, A. (2020). Energy Conscious Packet Transmission in Wireless Networks Using Trust Based Mechanism: A Cognitive Approach. In P. Singh, B. Bhargava, M. Paprzycki, N. Kaushal, & W. C. Hong (Eds.), *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's. Advances in Intelligent Systems and Computing* (Vol. 1132). Springer. doi:10.1007/978-3-030-40305-8_11

Biswas, S., & Nag, T. (2014). Trust Based Energy Efficient Detection and Avoidance of Black Hole Attack to Ensure Secure Routing in MANET. IEEE conference on Applications and Innovations in Mobile Computing (AIMoC), 157-164. doi:10.1109/AIMOC.2014.6785535

Cai, R. J., Li, X. J., & Chong, P. H. J. (2018). *An Evolutionary Self-Cooperative Trust Scheme against Routing Disruptions in MANETs.* IEEE. 10.1109/TMC.2018.2828814

Chen, J., Mao, G., Li, C., & Zhang, D. (2020). A topological approach to secure message dissemination in vehicular networks. *IEEE Transactions on Intelligent Transportation Systems*, *21*(1), 135–148. doi:10.1109/TITS.2018.2889746

Gupta, P., Goel, P., Varshney, P., & Tyagi, N. (2019). Reliability factor based AODV protocol: Prevention of Blackhole attack. In Smart innovations in communication and computational sciences, Advances in Intelligent Systems and Computing 851. Springer Singapore. doi:10.1007/978-981-13-2414-7_26

Hammamouche, A., Omar, M., Djebari, N., & Tari, A. (2018). Lightweight reputation-based approach against simple and cooperative black-hole attacks for MANET. *J Inf Secur Appl*, *43*, 12–20. doi:10.1016/j.jisa.2018.10.004

Huang, S., Liu, A., Zhang, S., Wang, T., & Xiong, N. (2020). BD-VTE: A novel baseline data based verifiable trust evaluation scheme for smart network systems. *IEEE Transactions on Network Science and Engineering*. Advance online publication. doi:10.1109/TNSE.2020.3014455

Jiang, B., Huang, G., Wang, T., Gui, J., & Zhu, X. (2020). Trust based energy efficient data collection with unmanned aerial vehicle in edge network. *Trans Emerging Tel Tech*, e3942. 10.1002/ett.3942

Josephine, J. A., & Senthilkumar, S. (2020). Tanimoto Support Vector Regressive Linear Program Boost Based Node Trust Evaluation for Secure Communication in MANET. *Wireless Personal Communications*. Advance online publication. doi:10.1007/s11277-020-07209-1

Khan, F. A., Imran, M., Abbas, H., & Durad, M. H. (2017). A detection and prevention system against collaborative attacks in mobile ad hoc networks. *Future Generation Computer Systems*, *68*, 416–427. doi:10.1016/j.future.2016.07.010

Khanna, M., & Sachdeva, M. (2020). BEST: Battery, Efficiency and Stability based trust mechanism using enhanced AODV for mitigation of Blackhole attack and its variants in MANETs. *Ad-Hoc & Sensor Wireless Networks*, *46*(3/4), 215–264. https://www.oldcitypublishing.com/journals/ahswn-home/ahswn-issue-contents/ahswn-volume-46-number-3-2020/18830-2/

Khanna, N., & Sachdeva, M. (2019). A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs. *Computer Science Review*, *32*(May), 24–44. doi:10.1016/j.cosrev.2019.03.001

Khanna, N., & Sachdeva, M. (2019). Study of trust-based mechanism and its component model in MANET: Current research state, issues, and future recommendation. *International Journal of Communication Systems*, *4012*(12), e4012. Advance online publication. doi:10.1002/dac.4012

Kollati, V.K., & Somasundaram, K. (2017). IBFWA: Integrated bloom filter in watchdog algorithm for hybrid Blackhole attack detection in MANET. *Information Security Journal: A Global Perspective, 26*(1), 49-60. .10.1080/19393555.2016.1274805

Manoranjini, J., Chandrasekar, A., & Jothi, S. (2019). Improved QoS and avoidance of Blackhole attacks in MANET using trust detection framework. *Automatika (Zagreb)*, *60*(3), 274–284. doi:10.1080/00051144.2019.1576965

Mayti, M., Khatoun, R., Begriche, Y., Khoukhi, L., & Gaiti, D. (2017). A stochastic approach for packet dropping attacks detection in mobile ad hoc networks, Comput. *Netw, Elsevier*, *121*, 53–64. doi:10.1016/j.comnet.2017.04.027

Merlin, R. T., & Ravi, R. (2019). Novel trust based energy aware routing mechanism for mitigation of Blackhole attacks in MANET. *Wireless Personal Communications*, *104*(4), 1599–1636. Advance online publication. doi:10.1007/s11277-019-06120-8

Mohanpriya, M., & Krishnamurthi, I. (2014). Trust Based DSR Routing Protocol for Mitigating Cooperative Black Hole Attacks in Ad Hoc Networks. *Arabian Journal for Science and Engineering*, *39*(3), 1825–1833. doi:10.1007/s13369-013-0764-1

Moussaoui, A., Semchedine, F., & Boukerram, A. (2014). A link-state QoS routing protocol based on link stability for Mobile Ad hoc Networks. *Journal of Network and Computer Applications*, *39*(3), 117–125. doi:10.1016/j.jnca.2013.05.014

Rajesh Babu, M., & Usha, G. (2016). A novel honeypot based detection and isolation approach (NHBADI) to detect and isolate Blackhole attacks in MANET. *Wireless Personal Communications*, *90*(2), 831–845. doi:10.1007/s11277-016-3229-5

Salman, M. S., Zhu, N., He, J., Zardari, Z. A., Memon, M. Q., & Hussain, M. I. (2018). An Efficient Trust-Based Scheme for Secure and Quality of Service Routing in MANETs. *Future Internet*, *2018*(10), 16. doi:10.3390/fi10020016

Sethuraman, P., & Kannan, N. (2014). Refined trust energy-ad hoc on demand distance vector (ReTE-AODV) routing algorithm for secured routing in MANET. *Wireless Netw*, 157-164. 10.1007/s11276-016-1284-1

Shanthi, K., Murugan, D., & Ganesh Kumar, T. (2018). Trust-based intrusion detection with secure key management integrated into MANET. *Information Security Journal: A Global Perspective, 27*(4), 183-191. .10.1080/19393555.2018.1505007

Singh, S., Bhasin, A., & Kalia, A. (2021). Capitulation of mitigation techniques of packet drop attacks in MANET to foreground nuances and ascertain trends. *International Journal of Communication Systems*, *34*(10), e4822. doi:10.1002/dac.4822

Subba, B., Biswas, S., & Karmakar, S. (2015). Intrusion detection in Mobile ad-hoc networks: Bayesian game formulation. J Eng Sci Technol, 19(2), 782-799. doi:10.1016/j.jestch.2015.11.001

Subramaniyan, S., Johnson, W., & Subramaniyan, K. (2014). A distributed framework for detecting selfish nodes in MANET using Record- and Trust-Based Detection (RTBD) technique. *EURASIP Journal on Wireless Communications and Networking*, *205*(1), 1–10. doi:10.1186/1687-1499-2014-205

Tripathy, B.K., Jena, S.K., Reddy, V., Das, S., & Panda, S. (2020). A novel communication framework between MANET and WSN in IoT based smart environment. *Int J Inf Tecnol.* 10.1007/s41870-020-00520-x

Usha, G., Rajesh Babu, M., & Kumar, S. S. (2017). Dynamic anomaly detection using cross layer security in MANET. *Computers & Electrical Engineering*, *59*, 231–241. doi:10.1016/j.compeleceng.2016.12.002

Wadhwani, G. K., Khatri, S. K., & Mutto, S. K. (2020). Trust framework for attack resilience in MANET using AODV. *Journal of Discrete Mathematical Sciences and Cryptography*, *23*(1), 209–220. doi:10.1080/09720529.2020.1721885

Wei, Z., Tang, H., Yu, F. R., Wang, M., & Mason, P. (2014). Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. *IEEE Transactions on Vehicular Technology*, *63*(9), 4647–4658. doi:10.1109/TVT.2014.2313865

Xia, H., Yu, J., Tian, C., Pan, Z., & Sha, E. (2015). Light-weight Trust-enhanced on-demand Multi-path Routing in Mobile Ad-hoc Networks. *Journal of Network and Computer Applications*. doi:10.1016/j.camwa.2012.03.023

Zhang, D., Gong, C., Jiang, K., Zhang, X., & Zhang, T. (2019). A kind of new method of intelligent trust engineering metrics (ITEM) for application of mobile ad-hoc network. *Engineering Computations*, *37*(5), 1617–1643. doi:10.1108/EC-12-2018-0579

Zhang, D., Zhu, Y., Zhao, C., & Dai, W. (2012). A new constructing approach for a weighted topology of wireless sensor networks based on local-world theory for the Internet of Things (IOT). *Computers & Mathematics with Applications (Oxford, England)*, *64*(5), 1044–1055. doi:10.1016/j.camwa.2012.03.023

Zhao, D., Ma, Z., & Zhang, D. (2016). A Distributed and Adaptive Trust Evaluation Algorithm for MANET. ACM. doi:10.1145/2988272.2990297

Nitin Khanna received the M. Tech. Degree in Computer Science and Engineering from Punjab Technical University, Jalandhar, Punjab, in 2015, Currently, Currently, he is pursuing Ph.D. in Computer Science & Engineering from IKGPTU, Kapurthala, India and working as Assistant Professor in Computer Science department at Kanya Maha Vidyalaya, India. His area of research is in the field of ad-hoc networks and security mechanisms. He has published 14 Research and review papers in different International Journals and Conferences.

Sandeep Singh received M.C.A degree from Punjab technical university, Jalandhar, India in 2004. He is currently working as an assistant professor at Lyallpur khalsa college, Jalandhar, India and currently pursuing Ph.D. from CT university Ludhiana, India. His current research interest includes wireless networks and machine learning.

Anshu Bhasin received Ph.D. degree in Computer Science and Engg. She has teaching experience of more than 20 years. She is currently working as assistant professor in I.K. Gujral Punjab technical university, main campus Kapurthala, India. She has published many research papers in reputed journals. She also authored two books. Her specializations include Computer Networks, Fiber Optics based Networks, Optimization Techniques using heuristics.

Kamal Malik currently works at the School of Engineering and Technology, CT University, Ludhiana. Kamal is doing her research in Databases, Data Mining, Artificial Intelligence, Machine Learning, Deep Learning etc. Their most recent publication is 'BDaaS: Overview & Synchronization Issue, Challenge Resolved Using Lamport's Logical Clock'.'