ENHANCED CLUSTER BASED TRUST MANAGEMENT FRAMEWORK FOR MOBILE AD HOC NETWORKS

MALIK NASERELDIN AHMED ABDELRAHMAN

A thesis submitted in fulfilment of the

requirements for the award of the degree of

Doctor of Philosophy (Computer Science)

School of Computing

Faculty of Engineering

Universiti Teknologi Malaysia

JANUARY 2019

To the spirit of my beloved wife.

ACKNOWLEDGEMENT

First and foremost, praises and thanks to the Allah, the Almighty, for providing me knowledge, guidance, and patience to achieve this goal. I would like to express my deep and sincere gratitude to my research supervisor, **Prof. Dr. Abdul Hanan Abdullah**, for giving me the opportunity to do research and providing invaluable guidance throughout this research. It was a great privilege and honor to work and study under his guidance. It would have been very difficult to complete this research successfully without his suggestions and thoughts. UTM management is highly appreciated for providing research incentives during this program. The members of Pervasive Computing Research Group are appreciated for their intellectual discussion and input in this thesis.

I am extremely grateful to my parents for their love, prayers, care, and sacrifices for educating and preparing me for my future. I owe my deepest gratitude towards my wife for her eternal support and understanding of my goals and aspirations. Her infallible love and support have always been my strength. I am thankful to my children Hatoon, Hadeel and Albarra for giving me happiness during my study. I show profound appreciation to my friend Dr. Haitham Ahmed Jamil for his helping and supporting during my study.

ABSTRACT

Trust management in decentralized networks and MANETs are much more complicated than the traditional access point based on wireless networks. The nodes in MANETs are used to provide trust information or evidence to find trustworthy nodes. However, the trust evaluation procedure depends on the local information due to its limited resources. In a trust management framework, there are issues to be resolved that include inefficient monitoring system with trust, inaccuracy in trust computation assign and lack of path selection based on trust. Therefore, in this research, a Trust Management Framework (TMF) was developed to address the aforementioned issues. The framework has the capability to monitor the network, assign trust values, and select an appropriate path for the transmission of packets among nodes which depends on the assignment of trust values. The TMF provides a secure cluster-based trust management to monitor the network that minimizes network overhead, improves path selection based on trust evaluation, and assigns trust for clusters-nodes with improved packet delivery ratio and delay. The performance of the TMF was assessed by performing simulation with Network Simulator version 2 (NS2). The results of the framework were compared with the state-of-the-art frameworks such as Requirement for Neural TMF (RNTMF), Recommendation Trust Framework with Defence Framework (RTMD), and Energy Efficient Secure Dynamic Source Routing (EESDSR). The results demonstrated that the Packets Delivery Ratio (PDR) of the TMF was 25.2% better than RNTMF, 21.4% better than RTMD, and 18.4% better than EESDSR. The overhead of the TMF was 4.5% less than RNTMF, 23.2% less than RTMD, and 26.8% less than EESDSR. The findings showed that TMF has better performance in terms of trust management in MANETs.

ABSTRAK

Pengurusan kepercayaan dalam rangkaian terdesentralisasi dan MANET adalah jauh lebih rumit daripada jalur akses tradisional berdasarkan rangkaian tanpa wayar. Nod di MANETs digunakan untuk memberi maklumat kepercayaan atau bukti untuk mencari nod yang boleh dipercayai. Walau bagaimanapun, prosedur penilaian kepercayaan bergantung kepada maklumat setempat disebabkan oleh sumber yang terhad. Dalam rangka kerja pengurusan kepercayaan, ada masalah yang harus diselesaikan termasuk sistem pemantauan yang tidak cekap dengan kepercayaan, ketidaktepatan dalam pengiraan perhitungan kepercayaan dan kekurangan pemilihan jalan berdasarkan kepercayaan. Oleh itu, dalam kajian ini, Rangka Kerja Pengurusan Amanah (TMF) telah dibangunkan untuk menangani isu-isu tersebut. Rangka kerja ini mempunyai keupayaan untuk memantau rangkaian, menetapkan nilai kepercayaan, dan memilih jalan yang sesuai untuk penghantaran paket di antara nod yang bergantung pada tugasan nilai kepercayaan. TMF menyediakan pengurusan kepercayaan berasaskan kluster yang selamat untuk memantau rangkaian yang meminimumkan overhed rangkaian, meningkatkan pemilihan laluan berdasarkan penilaian kepercayaan, dan memberikan kepercayaan kepada nod kluster dengan nisbah penghantaran paket yang lebih baik dan mengurangkan kelewatan. Prestasi TMF dinilai dengan melakukan simulasi dengan *Network Simulator* versi 2 (NS2). Hasil rangka kerja itu dibandingkan dengan rangka kerja terkini seperti Keperluan untuk Radiasi TMF (RNTMF), Rangka Kerja Amalan Rekomendasi dengan Rangka Kerja Pertahanan (RTMD), dan Laluan Sumber Dinamik keselamatan Tenaga Berkesan (EESDSR). Dapatan menunjukkan bahawa Nisbah Penghantaran Paket (PDR) TMF adalah 25.2% lebih baik daripada RNTMF, 21.4% lebih baik daripada RTMD, dan 18.4% lebih baik daripada EESDSR. Overhed TMF adalah 4.5% kurang daripada RNTMF, 23.2% kurang daripada RTMD, dan 26.8% kurang daripada EESDSR. Dapatan menunjukkan bahawa TMF mempunyai prestasi yang lebih baik dari segi pengurusan kepercayaan bagi MANET.

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AODV	-	Ad hoc On-Demand Distance Vector
CBRP	-	Cluster-Based Routing Protocol
CF	-	Collaborative Filtering
DoS	-	Denial of Service
DSR	-	Dynamic Source Routing
EESDSR	-	Energy Efficient Secure Dynamic Source Routing
HB	-	Interaction History stored in Buffer
IDS	-	Intrusion Detection System
IH	-	Interaction History
INFO	-	Trust Information
MANET	-	Mobile Ad hoc Network
NMST	-	Network Monitoring Scheme for Trust
NS2	-	Network Simulator 2
OSI	-	Open System Interconnection
PDR	-	Packet Delivery Ratio
RNTMF	-	Requirement for Neutral Trust Management Framework
RPST	-	Route Path Selection considering Trust
RREP	-	Route Reply
RREQ	-	Route Request
RTMD	-	Recommendation Trust Framework with Defense Framework
SDSR	-	Secure Dynamic Source Routing

SK	-	Symmetric secret Key
TA	-	Cluster Head
TCAS	-	Trust Calculation and Assignment Scheme
TEs	-	Trust Evaluators
TETBL	-	Trust Evaluation Table
TMFC	-	Trust Management Framework based on Clustering

LIST OF SYMBOLS

$Sim\ (i,j)$	-	The similarity of recommender node i and node j
P_{im}	-	The prediction for cooperative node i for rating m
K	-	The set of most similar neighborhood nodes
Y_c	-	Char ratio for component c
r_u	-	Rating Average
uth	-	User Rating.
PS	-	Number of data Packet Sent.
PR	-	Number of data Packet Received.
C_P	-	Control Packet transmitted in the network
D_P	-	Data Packet transmitted in the network
$A_{vg}(t)$	-	Average Time for total packet transmitted
$\overline{T_{*i}}$	-	Vector dot-product operation
t_v	-	Average of the Vth user's rating
n_i	-	A node i in the network
$Max(\sum S_j)$	-	Total number of successful interaction
TT_{nij}	-	Recommendation by recommender nj for the node ni
$TAinit$	-	Initial Cluster Head
$T_n i$	-	Initial trust value
n_j	-	A node j in the network
TT_{n_p}	-	Average of the p^{th} recommender ratings

t_0	-	Starting time
$t = (t_n\, t_0\,)$	-	Interval of recommenders ratings
$l(t)$	-	Forgetting ability of the function.
W_{ij}	-	Weight denoting the degree of a recommender rating that declined.

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Overview

The concept of Mobile Ad hoc Networks (MANETs) is considered to be a paradigm that does not utilize a stand aside infrastructure for communication. The MANETs are sets of mobile devices that interconnect between themselves using a wireless antenna in order to share resources. Looking at the non-centralized pattern of MANETs, the interaction between nodes is very paramount to offer network operations such as data routing. Conversely, during interaction among nodes, some nodes might take advantage of the absence of central manager to accomplish the malicious task (Sezer *et al.,* 2013). For example, a self-centered node might want to preserve its battery power by declining transmission of routing packets, since the node avoids the route that will enable its selection as a routing packet forwarder. Furthermore, a selfish attacker node might delete the received packet or differ the forwarding of the packet to disallow network services. Apparently, trusting a mischievous node can bring about unexpected problem including an increase in latency, increase in resource consumption and exposing node to attacks (Yi and Kravets, 2014). Therefore, there is a need for some sort of centralized controller, to monitor and guide the trust relationship between nodes of the network. MANETs are vulnerable to attacks and there is no solution to avoid such attacks. TMF can be employed in MANETs to find an alternative path to deliver the packets to the destination. It will recognize the trustworthy nodes in the networks using trust values or evidence (Movahedi and Hosseini, 2017). MANETs has become one of the most

established areas of research in recent years because of the challenges that are posed to its sustainability. In such environment, nodes are equipped with a wireless transceiver. Nodes can send/receive data as an end-host. They can also forward packets for other nodes as routers. Therefore, MANETs are decentralized and self-organized. The performance of the overall network system depends on the cooperation among all nodes in the network. However, due to the mobility nature of MANETs nodes, the network topology may change dynamically and unpredictably over time. In such case, some nodes may be compromised and behave selfishly or even act maliciously to disrupt the overall network operation due to the lack of standard infrastructure of the network (Wazid *et al*., 2011).

By deploying security measures, like cryptographic mechanisms, it can protect the correctness and integrity of the information transmitted in the system, but no security mechanisms can provide the trustworthiness of each party and predict their behaviors (Kim *et al*., 2008). Hence, the concept of trust in MANETs should be carefully defined in this regard; Trust is described as context-dependent which use meta-information about the circumstances in which information has been claimed (Xia *et al*., 2016). Current trust inference methods deployed in social network frameworks rely on simple trusts networks where the only trust between neighboring nodes is considered.

In the TMFs, there exist the following; trust formation component (Movahedi, *et al*., 2016), knowledge collection component and trust ranking computation component. The knowledge collection component provides systematic information regarding the behavior conduct of all nodes. The data gathered from the behavioral conduct are usually obtained from direct (local) or indirect (remote) source or even both (Wei *et al*., 2013). The local, which is the direct knowledge comprises of information that nodes have gathered by themselves on the conduct of their individual close neighbors. The remote knowledge, which is the indirect knowledge that is usually recommended, encompasses the view of a node that is not a neighbor node suggested for the trustworthiness of a particular node. The trust ranking computation component estimates a trust ranking for each node considering the gathered behavior

conduct data or trust confirmation. The obtained output is what that leads to the assignment of trust ranking, which represents the level of trust the node has. Further, the trust formation component employs the approximated trust ranking to carry out various network functions (Joshi and Mishra, 2016).

Evaluating trust within a dynamic MANETs environment is always challenging. MANETs do consist of different network properties compared to conventional infrastructure-based networks. In conventional infrastructure-based networks, two nodes may establish a trust relationship through a trusted third party, which is regarded as a recommender (Omar *et al*., 2012). This recommender acts as a central authority to supply the security certificates of verification for any requesting nodes. However, in a decentralized MANETs, such trusted recommender system does not exist. Therefore, each node must evaluate its own trust on other nodes individually in a timely fashion (Joshi and Mishra, 2016; Samreen and Narsimha, 2016; Laghari and Niazi, 2016).

Despite the fact that researchers have different disciplines in operationalizing trust, the trust framework is being increasingly adopted as an essential concept in designing and analyzing security problems in the distributed systems to guide decision making (Dong *et al.,* 2015). The existing trust frameworks designed mobile ad hoc networks requires improvement because the explicit mobility and dynamism features of MANETs have not been considered. Currently, how to define a dynamic trust evaluation framework to suit the outstanding features of MANETs is still an open research question and needs further discussion.

1.2 Problem Background and Motivation

Recent advances in networking technology have increased the potential for dynamic enterprise collaborations between an open set of entities on a global scale.

MANETs encounter problems in resource sharing as they are constructed by mobile nodes without any prior knowledge of the existing nodes, which may not be trustworthy. Trust management appears to be a promising approach to formalize trustworthiness among these anonymous nodes. Moreover, trust is regarded as a critical issue in respect of the design and deployment of security systems (Papadimitratos and Haas, 2016, Movahedi and Hosseini, 2017 and Prakash & Gupta, 2018).

In MANETs, trust evaluation can be applied for node verification, authentication, access control and trust-based routing protocols. By evaluating the trustworthiness of the related nodes, it does not only enhance the system security but also improves the overall performance in MANETs, by improving packet delivery ratio by reducing lost packets. (Liu *et al*., 2018). To define a dynamic trust evaluation framework for MANETs, there are several key factors that need to be considered. While, a numerous number of framework which are trusted managemental in the context of MANETs /based on network ,trust value calculation & assignment& path selection,/ on trust value have been proposed (Xia *et al.,* 2016a). Looking at the most current node-based-trust- managemental frameworks, each node entities assesses the trust ranking of its corresponding neighbors by using watchdog system. This watch dog system that employs an unrestrained style of the wireless network interface (Chauhan *et al.,* 2015; Li and Li, 2013; Naseer and Mahmood, 2015). It also performs the function of maintenance of most currently sent data packets and further, matches them with obtained overheard data packets to understand if there exists a match, actually (Li *et al.,* 2008). The process in these approaches creates a communication overhead and the trust might not be genuine enough since a node can be compromised within a short period of time because of the dynamic nature of MANETs. In addition, the approach might increase the energy consumption of mobile nodes.

The existing framework, Autonomic Trust Monitoring Scheme Framework (ATMF) (Movahedi *et al.,* 2012), assesses the trust level of nodes by using local information obtained from closeby nodes. The local, which is the direct trust of the certain neighbor node is acquired by considering that proportion of the generated

packet to that of the forwarded packet by a particular neighbor. The node's trust view of a neighbor and the node which are not its direct neighbor are disseminated throughout the network by using a technique called piggybacking. Accordingly, the overall communication overhead created during the recommendation exchange in the network is constrained by the volume of data piggybacked to transport the data packets. The framework is protected to a location-area double-face selfish attack because of the exploitation of indirect information. Though, the user-area double-face selfish attack cannot be discovered, except, if a recommendation is obtained from the affected node. Moreover, the suggested framework is susceptible to bad-mouthing attack because there is no system considered to distinguish between false and correct recommendations.

The other framework, Future TMF (FTMF) (Li *et al.,* 2008) receives indirect information, which is local knowledge by employing a watchdog system, whereas recommendations are disseminated via flooding method. An acceptance node assesses the confidence of a recommendation by employing nonconformity test and employs the trust ranking of the recommender node as, weight value, which shows the reputation of its recommendation. However, FTMF can unravel double-face behavior conducts by employing recommendations. It can also, repel dissident bad mouthing attacks considering the proposed nonconformity test. Interestingly, another dishonest model called Dishonesty Recommendations Detections Model with Framework (DRDMF) has been suggested by Lupia and De Rango, (2016), as an extension of Iltaf *et al.* (2013), is developed mainly to unravel deceitful trust recommendations. To attain the aforementioned aim, recommendations obtained by the node with low trustworthy value are termed as a dishonest recommendation. Furthermore, a recommendation suggestion, that is highly varying from the actual mean trust value is termed as dishonest irrespective of the trustworthy reputation of its recommender. The suggested system is not suitable for unravelling the bad mouthing behavioral conduct in multiple attack environment settings, where a higher varying recommendation might occur by a specific affected node of a double face attack. In the existing MANETs routing trust frameworks, the components including a monitoring system for a network, computation of trust value for assignment and path selection based on trust are usually

the major elements of the framework. However, all of these components need to be enhanced.

The following sub-sections discuss in detail on the main issues related to the existing TMFs and the appropriate path selection approaches in MANETs.

1.2.1 Inefficient monitoring system in MANETs

The inefficient monitoring system will allow intruders to inject more number of malicious nodes. The existing frameworks such as RNTMF and EESDSR are providing a good monitoring system but lacks in packets delivery ratio. It produces a high network overhead and more delayed output. Recent studies in MANETs have suggested that the trust framework to monitor MANETs, the trust values is used to improve the level of monitoring system. RNTMF, RTMD, FTMF, and EESDSR are also having inefficient monitoring system. The existing framework does not concentrate on trust establishment. The FTMF has objective based trust framework. It has followed a Bayesian approach for the trust assignment to find trustworthy nodes. It has loopholes for the intruders to enter into the network. It has argued that the framework is immune to bad mouthing attacks but there is no explanation for it.

Gosh *et al*. (2005) has proposed enhancement of trust management by introducing confidence level of trust for network monitoring of malicious activities. The trust value is assessed by assigning weight to the confidence level. The trust is estimated in a fully distributed manner, which offers a generic framework for routing protocols that do not consider a trust. However, the frequency of forwarding packets is not considered for assessing each nodes' confidence level. Further, Khan *et al*. (2016) have suggested a multi-attribute framework for trust, to handle the problem of insufficient trust parameters considered for network monitoring. The attributes include data packet forwarding, control packets generation and control packet forwarding. The framework considers direct surveillance using watchdog. In this, second-hand

information only is considered from the watchdog nodes, which has a higher trust value above a certain threshold. However, a relatively high network overhead might occur due to distributed inter-node assessment.

Bharathi *et al*. (2018) have proposed an intrusion detection framework based on Genetic algorithm (GA). The optimized trust value method is used to monitor the nodes in the network. The trust values were considered as the objective values of chromosomes. The method did not consider any deep interaction between nodes and it produced a high network overhead.

Li and Li, (2013) have proposed a design Requirement for Neutral TMF in MANETs (RNTMF). The framework is suggested in order to address the free-rider issue in the ad hoc peer-to-peer network. The framework encourages cooperation between nodes to avoid free-riders. The component of the framework includes trust propagation, trust calculation, trust enforcement and trust definition. The trust propagation is for monitoring, which is based on Initial Trust Form (ITF). ITF is the trust observation gathered by different nodes in the network. The trust calculation involves trust value, confidence value and trustworthiness evaluation. The trust enforcement component is mandated by using bloom filter for trustworthy nodes' list sharing. However, the trust propagation, that is, the monitoring component in this proposal only, is considered as a second-hand information, which might not be sufficient enough for the trust establishment. Because the expiry time for old observation has not been adequately mapped to the probability of node mobility. Therefore, the trust might not be actual, as a node, it can be compromised within a short period of time. In addition, high network overhead is generated due to the maintenance of currently sent packet and comparison of the packets with the overhead packet to see if there is a match.

The process in these approaches creates communication overhead and the trust might not be genuine, since a node can be compromised within a short period due to

the dynamic nature of MANETs. In addition, the approach might increase the energy consumption of mobile nodes.

1.2.2 Inaccurate Trust Computation Assignments

The approaches employed in the existing trust value computation are employed to gather a calculated direct and indirect trust values from the communicating nodes that already have a trust relationship. Examples of such studies are discussed subsequently. Baras and Jiang (2004) presented a distributed trust computation framework by employing random theory and graph theory for addressing inefficient trust computation and nodes' interaction in MANETs. The approach employs a concept of non-static collaborative games. It recognizes how a state transition from distrusted to trusted state occur considering non-static topology. The state transitions are related to node mobility and the topology of MANETs. The transition process is used for the preliminary trust establishment. The trust relationship is in three folds, that includes i) care, ii) no and iii) yes. The main focus is to maintain a steady node behaviour in MANETs. The trust variable should be continuous with a frequent update in trust values.

A quantitative framework approach based on ordered stochastic Petri-nets for addressing the problem of trust establishment computation without previous interaction (Cho *et al.,* 2009), both direct and indirect observation recommendation approach is employed. The trust property is considered based on dynamicity weighted transitivity with context-dependency asymmetric subjectivity, conversely, lack of computing of non-cooperating nodes, also, the feasibility needs to be determined.

A distributed trust mechanism that considers the energy of mobile nodes has been proposed for detection of the unpredictive malicious behavior of a node in MANETs (Kukreja *et al.,* 2015). The solution is based on enhancing security in Dynamic Source Routing (DSR) protocol. The protocol considers malicious

behavioral exhibitions of nodes. For example dropping data packets, dropping control packets, malicious topology changes, and gray hole. However, the mechanism and the protocol suffers from the incomplete interaction of nodes. Considering the aforementioned approaches, there is a need for improving the computation in the trust framework in order to minimize and the complexity, which causes routing overhead. Also, the lack of considering continuous variable based dynamic MANETs topology. Consequently, the energy consumption of the mobile nodes will come down if the trust value computation is improved.

1.2.3 Lack of Existing Work that Consider Trust in Path Selection

In the previous studies, the trust value of nodes is computed in a distributed manner. Path selection, considering trust in a non-grouped distributed manner may generate a lot of routing overhead. Thus, the most suitable path may not be selected. By the way, a trust framework that considers the use of a secure public key for authentication services has been suggested in order to avert dissemination of untrue public key from mischievous nodes. The framework employs distributed trust-based authentication with direct surveillance recommendation. Conversely, this study does not consider dynamic group variation based on MANETs topology behavior. Further, Ayachi *et al.* (2009) have presented an implicit trust correlation in AODV. In this, nodes utilize the trust correlation to segregate mischievous nodes to secure routing. It works in such a way that nodes can overhear neighbors' activities such as transmission, which based on that, they can create a neighbor routing table. Further, it checks for the disparity from normal behavior. Their framework can detect mischievous behaviors including modification, replication, and forgery of the message. However, monitoring behaviors considering competency and intimacy need tobe considered.

Adnane *et al.* (2009) suggested trust-based countermeasures to avoid mischievous nodes by extending Optimized LinkState Routing (OLSR). In this protocol, secure routing route paths are provided by recognizing mischievous nodes.

The protocol focuses on preventing usurpation of node distinctiveness. Performance analysis considering other kinds of attacks have not been investigated.

The aim is to ascertain and filter the ingenuity of second-hand information which is very much significant. Thus, shabut *et al.* (2015) suggested a protective trust system named the Recommendation Trust Framework wiasc Defense Framework (RTMD), which is centered on three constraints including confidence value, deviations in opinions and closeness value. The confidence value, indicates a number of interactions between an assessed node and a recommender node. The deviations, indicates the opinions of assessing node and recommender node. The closeness value, represents the distance of how closed an assessing node is to a recommender node. Considering the aforesaid constraints, an assessing node sieves the second-hand information in the suggested trust framework. Conversely, considering some situations in the suggested framework, the second-hand information sieving mechanism might not perform efficiently. For instance, when recommender nodes send a bad reputation value of the mischievous node to an assessing node, while the assessing node has good reputation value about the mischievous node based on first-hand information. Thus, this kind of recommendations is sieved out for the reason that there is a deviation in the value of trust. Therefore, that kind of good node might be selected.

1.3 Problem Statement

In trust management, Bayesian approach is used to calculate the trust values in the network. In general, Bayesian approach is computationally intensive. Some studies have proved that the model has occupied more memory to generate results for large dataset. The FTMF has used exponential decrease method to expire old behaviours of nodes but practically not possible.

The mobility of nodes between clusters in MANETs is one of the significant challenges to TMF. A recommender is necessary to intimate nodes about the entry of

new nodes into the network. Selection of nodes should not be partial, both trust values and recommenders feedback are taken into consideration. Existing frameworks are lacking in the selection of nodes. The concept of collaborative filtering can be implemented to address the problems in the selection of nodes.

Trust management system should not be attacked or easily subverted. The TMF has to face more challenges in MANETs. It has to monitor each node in the network. The weak security in trust management can lead to huge damage to the nodes in the networks. Existing studies focus on threat models and specific attacks on ad – hoc routing protocols. The studies do not give any importance to such attacks on trust management system.

Packets delivery ratio (PDR) indicates the successful transmission of messages in MANETs. Existing frameworks did not produce a better PDR, indicates its poor performance. The data accuracy of CF recommender system shows its capability of handling trust values. Trust values should not be shared by the recommenders. The improvement can be done on CF recommender system by partitioning the collaborative trust rating into distributed trust tables. This research explores a node-based TMF partitioning recommendation system of collaborative trust ratings, where the ratings are clustered according to the Interaction Histories (IH) and current trust value of the node in question.

The proposed framework employs both direct, which is local and indirect, which is remote information to unravel double face attacks by monitoring the overall network. The proposed framework has the ability to address the issues in the security and improve the overall performance of TMF.

1.4 Research Questions

Based on the discussion provided in Section 1.2. The research questions are formulated as follows:

i. How to enhance Network Monitoring System based on Trust (NMST) Management Framework for MANETs, in order to minimize network overhead?
ii. How to develop an integrated Trust Calculation and Assignment Scheme (TCAS) for Trust Management Framework to achieve accurate trust value and minimize computation overhead?
iii. How to develop a Route Path Selection and establishment based on Trust (RPST) clustering for the Trust Management Framework in order to minimize delay and improve packet delivery ratio?

1.5 Research Objectives

The aim of this research is to develop Trust Management Framework based on Clustering (TMFC) that is capable of securing nodes in MANETs. The framework will have the capability of monitoring the network, calculation trust value assignment and selecting the appropriates path for packets transmission among nodes based on trust value assignment. The objectives of this research are as follows:

i. To enhance Network Monitoring System based on Trust (NMST) Management Framework for MANETs, in order to minimize network overhead.
ii. To develop an integrated Trust Calculation and Assignment Scheme (TCAS) for Trust Management Framework to achieve accurate trust value and minimize computation overhead.
iii. To develop a Route Path Selection and establishment based on Trust (RPST) clustering for the Trust Management Framework in order to minimize delay and improve packet delivery ratio.

1.6 Research Scope

In light of the questions raised and objectives defined in this study the boundary of has been limited in scope of performance of the TMF used in the MANETs. The study mainly focuses on node-based clustering trust management and a framework is proposed for MANETs. AODV protocol is used to carry out the cluster head algorithm. The framework uses local information as trust values. In this research, Clustering of nodes will divide the total number of nodes into clusters. The clustering technique has produced better results in the field of computer networks. At the same time, the increasing of nodes number in MANETs will not result in decreasing the performance. It is worth mentioning role of a recommender system in TMF is vital to evaluate the trustworthiness of the nodes in the network.

1.7 Thesis Strategic

This thesis consists of six chapters as follows:

Chapter 1: Presents the introduction, background and general review of the problem. It discusses the trust-based management problems used for securing the route, and the viable path determination. Then it discusses the problem statement of this research and the objectives.

Chapter 2: Describes the literature review, discusses in-depth, the literature review of the review of the study. Different types of network monitors discussed in details, and then the following are discussed in details: the trust management in MANET, path selection based on trust, trust value calculation using a weighted clustering algorithm, and collaborative filtering.

Chapter 3: Explain the research methodology adopted in the trust-based management framework for secure routing in MANET. It includes the operational

framework used in the thesis for design and development. The performance evaluation of the research is presented in details at the end of this chapter.

Chapter 4: Presents the implementation process of the proposed trust management framework for MANETs; it discusses the design of the network monitoring, trust-based filtering technique for recommenders, recommender a list for Top Algorithm, and the cluster formation and cluster head (TA) selection algorithm.

Chapter 5: Presents the performance evaluation of the proposed framework, the performance and evaluation result of the proposed framework are discussed. The outcomes are analyzed in details and the comparison with the state-of-the-art.

Chapter 6: Summarizes the research work and future research directions.

REFERENCES

Abdul-Rahman, A. and Hailes, S. (2000). Supporting trust in virtual communities. In *System Sciences, 2000. In Proceedings of the 33rd Annual Hawaii International Conference on System Sciences.* 7-7 Jan. Maui, HI, USA. IEEE, 1-9.

Adnane, A., Bidan, C. and de Sousa Junior, R.T. (2009). August. Trust-based countermeasures for securing OLSR protocol. In *International Conference on Computational Science and Engineering*. 29-31 Aug. Vancouver, BC, Canada. IEEE, 745-752

Ayachi, M.A., Bidan, C., Abbes, T. and Bouhoula, A. (2009), August. Misbehavior detection using implicit trust relations in the AODV routing protocol. In *International Conference on Computational Science and Engineering.* 29-31 Aug. Vancouver, BC, Canada. IEEE, 802-808.

Bharathisindhu, P. and Brunda, S.S. (2018). An improved model based on genetic algorithm for detecting intrusion in mobile ad hoc network. *Cluster Computing*. Jan, 1-11.

Billieux, J., Maurage, P., Lopez-Fernandez, O., Kuss, D. J., and Griffiths, M. D. (2015). Can disordered mobile phone use be considered a behavioral addiction? an update on current evidence and a comprehensive framework for future research. *Current Addiction Reports.* 2(2), 156–162.

Buchegger, S. and Le Boudec, J.Y. (2002). Performance analysis of the CONFIDANT protocol. In *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. 9-11 June. Lausanne, Switzerland. ACM, 226-236.

Buchegger, S. and Le Boudec, J.Y. (2004). A robust reputation system for peer-to-peer and mobile ad-hoc networks. *In Proceedings of P2PEcon 2004 (No. LCA-CONF-2004-009)*. 3-11 June. Cambridge MA, U.S.A. Springer, 1-6.

Castelfranchi, C. and Falcone, R. (1998). Principles of trust for MAS: Cognitive anatomy, social importance, and quantification. In *Proceedings of International Conference on Multi Agent Systems*. 3-7 July. Paris, France. IEEE, 72-79.

Chauhan, A., Gupta, D., and Sah, M. K. (2015). Detection of packet dropping nodes in MANET using DSR routing protocol. *International Journal of Computer Applications*. 123(7), 11-16.

Cho, J.H. and Swami, A. (2009). Towards trust-based cognitive networks: A survey of trust management for mobile ad hoc networks. *In Proceedings of the 14th International Command and Control Research and Technology Symposium (ICCRTS)*. 15-17 June. Washington, DC. DTIC, 1-38.

Dong, P., Qian, H., Zhou, K., Lu, W., and Lan, S. (2015). A maximally radio-disjoint geographic multipath routing protocol for MANETs. *Annals of Telecommunications - Annales des Telecommunications*. 70(5), 207–220.

Douceur, J. R., Levin, D. M., Lorch, J. R., and Moscibroda, T. (2016). Trusted hardware component for distributed systems. Google Patents U.S. 9,455,992.

Elofson, G. (2013). Developing trust with intelligent. Trust and Deception in Virtual Societies, *Springer Science Business Media B.V. 2001*, Springer Dordrecht.

Ghosh, T., Pissinou, N. and Makki, K. (2005). Towards designing a trusted routing solution in mobile ad hoc networks. *Mobile Networks and Applications*, *10*(6), 985-995.

Griffiths, J.C., Du, E.Y., Burns, D.W. and Sezan, M.I. (2015). *Trust broker authentication method for mobile devices*. Google Patent U.S. 14,523,679.

Handy, M.J., Haase, M. and Timmermann, D. (2002). Low energy adaptive clustering hierarchy with deterministic cluster-head selection. In *Proceedings of the 4th International Workshop on Mobile and Wireless Communications Network.* 9-11 Sept. Stockholm, Sweden. IEEE, 368-372.

Iltaf, N., Ghafoor, A., and Zia, U. (2013). A mechanism for detecting dishonest recommendation in indirect trust computation. *EURASIP Journal on Wireless Communications and Networking*, 1(Dec), 1-13

Jain, A.K., Tokekar, V. and Shrivastava, S. (2016). Security Enhancement in MANETs Using Fuzzy-Based Trust Computation Against Black Hole Attacks. In *Proceedings of the 2nd International Conference on Information and Communication Technology*. 12-13 Dec. Singapore. Springer, 39-47.

Jiang, T. and Baras, J.S. (2004). Ant-based adaptive trust evidence distribution in MANET. In *Proceedings of the 24th International Workshops on Distributed Computing Systems*. 23-24 Mar. Hachioji, Tokyo, Japan. IEEE, 588-593.

Joshi, S. and Mishra, D. K. (2016). A roadmap towards trust management & privacy preservation in mobile ad hoc networks. In *Proceedings of International Conference*

on ICT in Business Industry & Government (ICTBIG). 18-19 Nov. Indore India. IEEE, 1-6.

Khan, M.S., Khan, M.I., Khalid, O., Azim, M. and Javaid, N. (2016). MATF: a multi-attribute trust framework for MANETs. *EURASIP Journal on Wireless* Communications and Networking, 1(Dec), 1-17.

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A trust-based consumer decision-making model in electronic commerce: The role of trust, perceived risk, and their antecedents. *Decision Support Systems.* 44(2), 544-564.

Kukreja, D., Dhurandher, S.K. and Reddy, B.V.R. (2015). Enhancing the security of dynamic source routing protocol using energy aware and distributed trust mechanism in MANETS. In *International Conference on Intelligent Distributed Computing.* 1-5 June, Switzerland. Springer, Cham, 83-94.

Laghari, S. and Niazi, M. A. (2016). Frameworking the internet of things, self-organizing and other complex adaptive communication networks: a cognitive agent-based computing approach. *PloS one*. 11(1) 1- 26.

Li, J., Li, R., and Kato, J. (2008). Future trust management framework for mobile ad hoc networks. *IEEE Communications Magazine*. 46(4), 108-114

Li, R. and Li, J. (2013). Requirements and design for neutral trust management framework in unstructured networks. *The Journal of Supercomputing.* 64(Nov), 702-716.

Liu, G., Yan, Z., & Pedrycz, W. (2018). Data collection for attack detection and security measurement in Mobile Ad Hoc Networks: A survey. *Journal of Network and Computer Applications*. 105(1), 105-122.

Lupia, A. and De Rango, F. (2016). Trust management using probabilistic energy-aware monitoring for intrusion detection in mobile ad-hoc networks. In *the Proceedings of International Conference on Wireless Telecommunications Symposium (WTS)*. 18-20 Apr. London, UK. IEEE, 1-6.

Marsh, S., Dibben, M., and Dwyer, N. (2016). The wisdom of being wise: A brief introduction to computational wisdom. *In Proceedings of the International Conference on Trust Management IFIP*. 18-22 July. Darmstadt, Germany. Springer, 137–145.

McKnight, D.H. and Chervany, N.L. (2002). What trust means in e-commerce What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce.* 6(2), 35-59.

Movahedi, Z. and Hosseini, Z. (2017). A green trust-distortion resistant trust management on mobile ad hoc networks. *International Journal of Communication Systems*. 30(16), 1-11.

Movahedi, Z., Nogueira, M., and Pujolle, G. (2012). An autonomic knowledge monitoring for trust management on mobile ad hoc networks. In *Proceedings of the International Conference on Wireless Communications and Networking (WCNC)*. 1-4 Apr. Shanghai, China. IEEE, 1898–1903.

Movahedi, Z., Hosseini, Z., Bayan, F., & Pujolle, G. (2016). Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey. *IEEE Communications Surveys & Tutorials*. 18(2), 1287-1309.

Naseer, S. and Mahmood, R. (2015). Intrusion detection techniques in mobile ad hoc networks: A review. *Lecture Notes on Information Theory*. 3(1), 52–55.

Ngai, E.C. and Lyu, M.R. (2004). Trust-and clustering-based authentication services in mobile ad hoc networks. In *Proceedings of the 24th International Conference Workshops on Distributed Computing Systems.* 23-24 Mar. Hachioji, Tokyo, Japan. IEEE, 582-587.

Omar, M., Challal, Y., & Bouabdallah, A. (2012). Certification-based trust models in mobile ad hoc networks: A survey and taxonomy. Journal of Network and Computer Applications. 35(1), 268-286.

Prakash, J., & Gupta, D. K. A Survey of Trust based Adaptive Gateway Discovery in MANET for Integrated Internet. *International Journal of Innovation and Advancement in Computer Science*. 6(9), 87-99.

Patwardhan, A., Parker, J., Iorga, M., Joshi, A., Karygiannis, T. and Yesha, Y. (2008). Threshold-based intrusion detection in ad hoc networks and secure AODV. *Ad Hoc Networks.* 6(4), 578-599.

Pirzada, A.A. and McDonald, C. (2006). Trust establishment in pure ad-hoc networks. *Wireless Personal Communications*. 37(2), 139-168.

Samreen, S. and Narsimha, G. (2016). Defense against on-off packet droppers in a trust management framework for a mobile ad hoc network. In *Proceedings of the International Conference on Internet of Things and Applications (IOTA).* 22-24 Jan. Pune, India. IEEE, 448–453.

Sezer, S., Scott-Hayward, S., Chouhan, P. K., Fraser, B., Lake, D., Finnegan, J., . . . Rao, N. (2013). Are we ready for SDN? Implementation challenges for software-defined networks. *IEEE Communications Magazine*. 51(7), 36-43.

Shabut, A.M., Dahal, K.P., Bista, S.K. and Awan, I.U. (2015). Recommendation based trust model with an effective defence scheme for MANETs. *IEEE Transactions on Mobile Computing*. 14(10), 2101-2115.

Sun, Y.L., Yu, W., Han, Z. and Liu, K.R. (2006). Information theoretic framework of trust modeling and evaluation for ad hoc networks. *IEEE Journal on Selected Areas in Communications*. 24(2), 305-317.

Velloso, P. B., Laufer, R. P., Cunha, D. D. O., Duarte, O. C. M., and Pujolle, G. (2010). Trust management in mobile ad hoc networks using a scalable maturity-based framework. *IEEE transactions on network and service management*. 7(3), 172–185.

Wei, Z., Tang, H., Yu, F.R. and Wang, M. (2013). Security enhancement for mobile ad hoc networks routing with OLSRv2. In *Proceedings of Mobile Multimedia/Image Processing, Security, and Applications Conference.* 28-28 May. Baltimore, Maryland, U.S.A. SPIE, 1-8.

Xia, H., Yu, J., Pan, Z.-k., Cheng, X.-g., and Sha, E. H.-M. (2016a). Applying trust enhancements to reactive routing protocols in mobile ad hoc networks. *Wireless Networks*, 22(7), 2239–2257.

Xia, H., Yu, J., Tian, C.-l., Pan, Z.-k., and Sha, E. (2016b). Light-weight trust-enhanced on-demand multi-path routing in mobile ad hoc networks. *Journal of Network and Computer Applications* 62(Feb), 112–127.

Zhou, L. and Haas, Z. J. (1999). Securing ad hoc networks. *IEEE Network.* 13(6), 24–30.