International Journal of Digital Information and Wireless Communications (IJDIWC) 9(3): 143-156
The Society of Digital Information and Wireless Communications, 2019 ISSN: 2225-658X (Online); ISSN 2412-6551 (Print)

An Application-centric Trust Management Framework for Mobile Ad Hoc Networks

Thulani Phakathi, Francis Lugayizi, B. Esiefarhenrhe, Bassey Isong
Department of Computer Science, North-West University
Private Bag x2046, Mmabatho, Mafikeng, South Africa
katshego@gmail.com{francis.lugayizi, bassey.isong, 25840525(@nwu.ac.za)}

***Abstract*— Trust is an important computer network concept and remains an issue not just in social platforms but also in networks in delivering Quality of service (QoS). Video Streaming has, over the years gained prominence in mobile and vehicular ad hoc networks, however, video streaming is faced with several challenges of being vulnerable to different attacks and poor QoS. This work proposed a robust and efficient trust management framework that eliminates poor QoS due to network detriments caused by the dynamic topology of a MANET. The trust framework aims to assist in node accountability and QoS attainment, i.e. it does not remove the dynamic topology issue but it strives to attain nodes' trustworthiness and excellent QoS despite the conditions set out against the network. The proposed trust framework is an application-centric trust management framework with distributed trust computations (AppTrusFram). It merges the concept of trust together with QoS in an application scenario. This work presented a theoretical-design solution to the topology-related issues and discussed issues found in other proposed solutions. The QoS evaluation conducted for low and high node density scenarios based on two routing protocols AODV and OLSR carrying video conference traffic (high quality). By using the framework and the establishment of a trust in the network, the achieved results proved its significance as delay periods were extremely low. The also results proved that OLSR performs better in high node densities and traffic as compared to AODV whose information overhead grows as the network density increases. The results showed an overall excellent QoS. A conclusion was drawn that OLSR needs constant topological update messages to perform well and this observation can be used as a future reference point to provide the best service in video streaming applications over MANETs**

Keywords*— *Routing protocols, MANETs, Trust framework, Video streaming, QoS.

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) also referred to as an infrastructure-less network [4] is a network technology that has gained significant attention in the research world in recent years due to related protocols challenges it faced. MANETs are an emerging technology that offers network users interactions without any central infrastructure irrespective of the geographical location of the users. MANETs have been an active area of research for the last few years and their growth is promoted by the growing need to provide the users with the network support at their own convenience [5]. The network is primarily useful in military and other tactical applications such as emergency rescue or exploration missions [6]. Their commercial success has been due to advances in wireless technology and several standards have been developed for routing in MANETs. The Internet Engineering Task Force (IETF) is responsible for regulating the new group for MANETs and IEEE standard 802.11 has contributed to research interest done with MANETs [4]. What also facilitated the explosive growth is the continued production of smaller and faster devices which makes MANETs the fastest growing network.

Today, MANETs are considered as a household technology service in the mobile network industry. Its growth has been commended globally and has attracted so much attention in recent years with the invention of Vehicular Ad Hoc Networks (VANETs) and its integration into the automotive industry. In particular, the fast demand for video streaming applications like video conferencing and video-on-demand are central to MANET technology. Researchers in recent studies have shown great interest in Quality of service (QoS) in the mobile network realm.

QoS is considered a set of service requirements that a network is required to meet in the movement of packet streams from the source to destination. With the explosive demand of QoS provisioning for evolving applications (e.g. video and voice), it is proportionally appropriate to ensure that these services are supported in ad hoc networking environments. In the field of telecommunications,

QoS was defined as a set of requirements on all the aspects of a connection, such as crosstalk, response time, loss, echo, signal-to-noise ratio, interrupts, frequency response, loudness levels, and so on. Moreover, QoS constitute the ability to proffer a different level of priority to different users, applications, or data flows, or to ascertain a precise performance level to a data flow [8]. However, in order to achieve QoS, the concept of routing is indispensable. Routing involves information movement in a network from a source to a destination [8]. During routing, at least one node within the network which acts as an intermediary is met during the information movement. Thus, routing can be used to determine optimal routing paths as well as the transfer of packets via an inter-network [9]. Moreover, routing may be either dynamic or static [9]. QoS is measured using specific metrics within the network such as bandwidth, jitter, delay, packet loss, etc.

In the realm of MANETs, the mobility of nodes, however, is rapid and unpredictable over time. MANETs, like all other wireless networks, are more vulnerable to attacks and other weaknesses as compared to wired networks. The limitations in MANETs become especially exacerbated in the multi-hop networks where multimedia streams suffer aggregate effects such as packet drop, propagation delay and jitter of each connected link along an end-to-end path. Due to node mobility, there are frequent route breaks which result in routing updating that is time-consuming. Consequently, packets might be lost in bursts for shorter periods of time since they are sent on non-working routes [7] which in turn impacts the QoS adversely.

Therefore, this paper proposes a robust and efficient trust management framework in an effort to eliminate the poor QoS due to network detriments caused by the dynamic topology of MANETs. The proposed trust framework is an application centric-framework that amalgamates the concept of trust together with QoS evaluation. The objective is not to remove the dynamic topology issues but it strives to attain nodes' trustworthiness and excellent QoS despite the conditions set out against the network. The proposed trust framework is called an application-centric trust management framework with distributed trust computations (AppTrusFram). Furthermore, we present solutions to the topology related issues provided by the proposed trust model and discussed issues in other proposed solutions.

This paper is organized as follows: Section II discusses the various routing protocols (RPs) in MANETs, Section III is on trust in MANETs and Section IV presents trust management frameworks studies while Section V presents the proposed framework.

2. ROUTING PROTOCOLS IN MANETS

This study focuses on reactive and proactive protocols which are the RPs that are based on topological information in MANETs as well as in VANETs [3][19][22]. Each is discussed as follows.

2.1 Proactive Protocols

These protocols operate by periodically trading control messages of known routes between all the network routers [5][6] [35]. Proactive routing protocols include DSDV, OLSR, Fishy State Routing (FSR) and so on. Thus, OLSR is the focus of this study.

a)OLSR protocol: In the OLSR protocol, every station found in the network chooses a neighboring node-set known as the multipoint relays (MPR), which rebroadcasts the packets in turn. To this end, neighboring nodes identified not found in the MPR set has the capability to only read and process the packets [5]. Moreover, OLSR retains tracks in the pathfinding table in order to proffer a route if necessary [8].

2.2 Reactive Protocols

These reactive protocols are also called on-demand protocols and include AODV, DSR, and TORA [22].

a)DSR protocol: In DSR, the discovery of route begins on-demand and the whole path to the destination is placed on the routing table other than using next-hop node as in the AODV. The packet header has the address of all the nodes in the transition needed by the packet to get to the destination node [10]. In addition, nodes can be dynamically discovered in a source route through complex networks hop to any terminus in VANETs by DSR. However, the protocol lacks the mechanism to identify unstable routes leading to

forwarding to the data packet to broken links [11]. In operations, DSR implements three unique techniques for controlling packets for path discovery and maintenance [10].

b) AODV protocol: AODV operates on a pattern known as hop-by-hop and uses flat routing tables having one entry per destination [11]. Unlike DSR, the AODV algorithm enables high mobility, dynamic, multi-hup and self-initiating routing among collaborating vehicles that are interested in ad-hoc network establishment and maintenance. In this case, routes can be acquired speedily for new destinations by mobile nodes without keeping routes in which commination is not active to destination.

c)TORA protocol: TORA protocol works on controlling the propagation of messages in the ever-changing ad-hoc networks. Nodes are known to clearly begin a query only when data is to be sent to a destination. In terms of performances, TORA performs much better as compared to that of DSR in a network [4]. According to Qureshi and Abdullah [4], the reason be due to the protocol's ability to minimize the communication overhead in a dynamic environment thus, making it more reliable for changing Ad-hoc networks. In addition, Palta and Goyal [9] stated that one good aspect in the design of TORA is that there is a localization of control messages to few node sets and the effective way link failures are handled.

3. TRUST IN MANETS

In this section, we present the nature of trust and related works on trust management in MANETs.

3.1 Trust Factor

The term "trust" is used in the perspective of how one party (normally referred to as trustor) is willing to rely on another party (may be referred to as trustee). It is greatly attributed to human beings and their relationships in social groups. However, in the Computer Science discipline, a trusted component has elements within itself that another component within the system can rely on. For instance, if component **A** trusts component **B**, this means that any violation of properties found in component **B**, will ultimately affect the correct operation of **A** - *dependency*. This, however, doesn't mean if **A** trusts **B**, then component **C** can trust **B**. In the realm of MANETs, due to its characteristics, trust management is required for participating nodes that communicate together in a network to provide a satisfactory or acceptable level of trust relationships among them without any previous interactions [1]. Nevertheless, trust management in MANETs are enormously challenging because of its dynamic nature and characteristics which is attributed to topology changes as well as uncertainty and incompleteness.

a)Direct Trust: In Kiefhaber *et al.* [20], direct trust is a form of trust which involves the experiences an entity has created directly with another entity it interacts with which is computed using trust value. Typically, trust values are computed using either the mean or weighted mean of previous experiences. Direct trust is application-centric or rather specific. The application has the decision to determine whether an interaction made by one entity to another was successful. Direct trust was chosen based on the merits that it is reliable in terms of rankings from confidence trust and reputation[20]. On the middleware level, which in this case is the application server, a node's reliability can be computed through observation of the message flow in the distributed system. initially, the Delayed-Ack mechanism was used and was later changed.

b)Topology Constraints in MANETs: A network topology that is trustworthy must be assured via the use of robust routing protocols in the ad hoc networking stream [1]. They are required because of the frequent routing updates caused by the dynamic nature and characteristics existing in MANETs. Providing QoS at a better scale in such environments is a huge challenge [4]. The existing stochastic nature of MANETs' quality of communications poses challenges in offering concrete guarantees on the applications computed in mobile devices. Thus, a QoS that is adaptive must be realized coupled with a strong trust relationship framework over the traditional methods reserving resources to support multimedia streaming services. But, due to the constant change in network topology, the issue of routing packets between nodes poses a great problem. Multicast routing also poses a challenge since the multicast tree ceases to be static since nodes in the network move randomly. The routes between nodes often have multiple hops which are considered complex than

its single counterpart. In MANETs, the nodes are mobile and this feature could result in nodes getting out of range within the network [4]. This causes frequent loss of links between nodes. That is, when nodes are in motion, the state of present node links are most susceptible to changes or possibly break. Re-routing is an alternative when routes are broken.

c)Trust and QoS: Trust and QoS have almost similar metrics in order to evaluate their efficiency. There are different ways to define trust. Trust is considered a directional relationship between two entities [17]. Though trust has been considered as a computational model, it is viewed differently by different research communities. QoS in MANET [8] which is a universally growing area. With the rapid advancements in multimedia technology today, there is an urgent need for mobile technology and real-time applications to strictly support QoS such as throughput, delay, energy consumption, jitter, etc. Trust and QoS share similar metrics e.g. delay, throughput and packet dropping rate. The correlation between these concepts exists not only through shared performance metrics but also the assurance of good service in the network for the end-user. QoS and Trust are what stand in between the network and the Applications/Users. It is not easy to provide QoS support without having the right QoS requirements. A particular level of trust must be established and that is, only trustworthy nodes that perform as desired will participate. Trust is dynamic [16] just like MANETs which have an ever-changing topology state. This means that the trust value should be based on temporary and yet local information. In addition to this, the trust value is different for similar nodes is different. This is influenced by that each node goes through different situations in terms of the dynamic topology.

4. RELATED WORKS ON TRUST MANAGEMENT FRAMEWORKS IN MANETS

Trust remains [1] a relevant subject within the research field and continues to attract interest from network analysts and developers. The notion of using Trust to eradicate security problems in networks has also been relevant in the research field. Ferdous *et al.* [12], proposed a novel approach to address problems by using trust as a metric. Their approach is based on the node's responsibility to build an acceptable trust level and monitoring [12]. Their work is based only at the node level and this paper seeks to go deeper into considering other factors like the QoS at the network and trust in the entire network. This means that a bridge between trust and QoS will be built in this paper.

Sen [17] proposed a reputation and trust-based security framework for MANETs that detect packet-dropping attacks launched by malicious and selfish nodes. The framework was based on a trust model that is based on the reputation of other network nodes. The study stated that MANETs are prone to security threats in which a node could hide its initial identity and disguisedly re-enter a network environment where users are penalized for behavior that seems selfish or malicious. The solutions proposed involved invoking a univocal relation between a terminal and the initial identity it assumed when it first enters the network [17]. The work was implemented for only small scale performances and not high scale. It was at a simulation area of 100*100m. DSR protocol is widely known for its scalability problem especially when the ad hoc network topology varies. Different results could have been achieved through the OLSR protocol or rather the TORA protocol which can evaluate either a proactive or even a reactive protocol.

Li *et al.* [14] also proposed a trust-based framework which can be incorporated with diverse single-copy data forwarding protocols in Opportunistic Networks (OppNets). It aimed at carrying out an in-depth assessment of the potential encountered for data delivery [18]. Their work aimed at counteracting arbitrarily forwarding attacks [18]. Zhang *et al.* [19] also focused on the problem of control delay-constrained topology having in mind, other problems like account delay and interference. The study proposed a cross-layer distributed algorithm known as an interference-based topology control algorithm for delay-constrained (ITCD) MANETs [18] while taking the interference and delay constraints into consideration. Additionally, the study investigated the effect of node mobility on the interference-based topology control algorithm where any node considered not stable is removed. The results obtained from the simulation performed showed that ITCD reduces the delay and in turn

also improves the performance effectively in delay-constrained mobile ad hoc networks.

Li and Kato [11] proposed an Objective Trust Management Framework (OTMF). The framework assessed nodes' trust and was used to compel nodes to collaborate in a manner that is normal. The framework was geared towards designing a robust and attack-resistant trust management framework to overcome vulnerabilities problems in the future. These vulnerabilities include not only topology-related or scalability-related vulnerabilities. Moreover, Shabut et al. [20] proposed a trust model that is recommendation-based. It has a defense mechanism that can dynamically filter out attacks using clustering techniques and the model was empirically evaluated. The empirical analysis demonstrated the attributes of robustness and accuracy in a MANET dynamic environment. However, the results, cannot be validated in an experimental process since the framework is based on recommendations. Thus, our proposed framework is one based on direct trust

Trust is an important feature in networks [10]. The nature of MANETs still makes the guarantee of efficient trust a complex task due to its highly dynamic topology constraints. The emergence of MANETs calls for the addressing of many problems perceived in networks and also optimizing some of the existing network resources [2]. The question that remains unresolved is "c*an trust be truly guaranteed in a MANETs?*" The answer to this question according to this study will be based on the QoS. Different authors have presented different trust frameworks. According to Li and Kato [11], existing trust frameworks are faced with great challenges under hostile environments, which can adversely affect their performance. This means that the reason most frameworks failed is that they did not address the problem of topology and its being dynamic in nature in these types of networks hence the need for robust frameworks that will be resistant and still get to give out optimum performance.

Ferdous *et al.* [12], also developed a simple node-based trust management technique for MANETs. It provides multiple standpoints of trust, its properties which are trusted metrics, and the insights into the customization the metrics meet the requirements and goals of the network trust management (NTM) scheme. Their future work was set to develop trust management mechanisms having the required attributes like scalability, adaptation to topology dynamics, and reliability [12]. A good scheme is one that encompasses all these characteristics in order to ensure trust in the network. Dynamically changing topology is one of the characteristics and limitations of MANETs. The most important aspect is achieving good QoS.

Thus, a robust and efficient trust management framework is needed to ensure nodes are trustworthy and prevent them from being selfish or performing selfishly as well as provide good QoS. This work seeks to close that gap by building a framework that not only looks at Trust but also with reference to video streaming applications in MANETs. Much concentration will be based on the achievement of trust between nodes of a network. Different network scenarios will be established, which means an outlook on performances, behavior and together with their quality of service of video streamed applications will be closely analyzed.

5. PROPOSED APPLICATION-CENTRIC TRUST FRAMEWORK

This section presents a high-level overview of the proposed trust management framework and the different components or technologies associated with it. It also presents assumptions that we made in connection with the framework.

5.1 System Overview

In this paper, we proposed an application-centric trust management framework with distributed trust computations (AppTrusFram). AppTrusFam is a video streaming application, a rising technology innovation in MANETs which may come in the form of low-resolution video or high-resolution video. The proposed framework involves the application server together with distributed trust computations. (See Fig. 1) The benefits are that it is a management system that is able to compute the end result which is QoS evaluation in the form of throughput, delay, and jitter and so on. In Fig. 1, the AppTrusFam involves neighboring nodes direct trust. The application server plays an important role in the attainment of excellent QoS and is built-in in every workstation since they act as its own router. This is because it encompasses features that involve security, diagnostics, and clustering. Distributed

trust computations are based on 'knowledge', 'recommendation' and 'experience'.

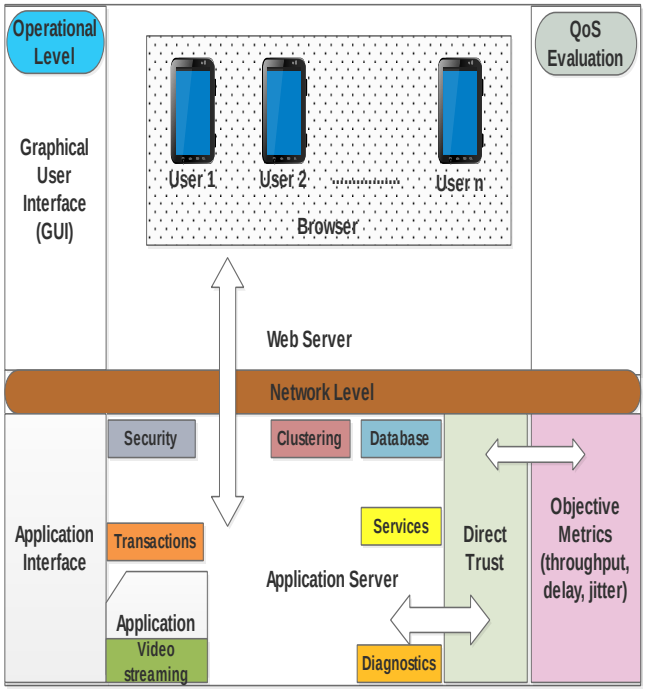

Fig. 1. Trust management architecture

The choice of direct trust is due to its versatility and its ability to sense neighboring nodes since MANET stations operate through WiFi or Bluetooth connectivity. On the other hand, the web-server is responsible for processing client requests and send responses via the HTTP protocol. Within the web-server lies the web browser, an application, which is responsible for retrieving, traversing and presenting HTTP requests onto stream(able) media in the World Wide Web.

6. AppTrusFram Components

AppTrusFram showed in Fig. 1 is video streaming which shows a link between direct trust and QoS metrics. The components are discussed as follows:

a)Application server: The Application server consists of the business logic and the application programs using various protocols. It also takes charge of all application operations that exist between users and an organization. It is able to deploy applications and it primarily acts as middleware, an abstraction and serves that facilitate the design, development, and integration of distributed applications in heterogeneous net-environments. In MANETs, the nodes are self-configuring, basically meaning they have their own internal application server.

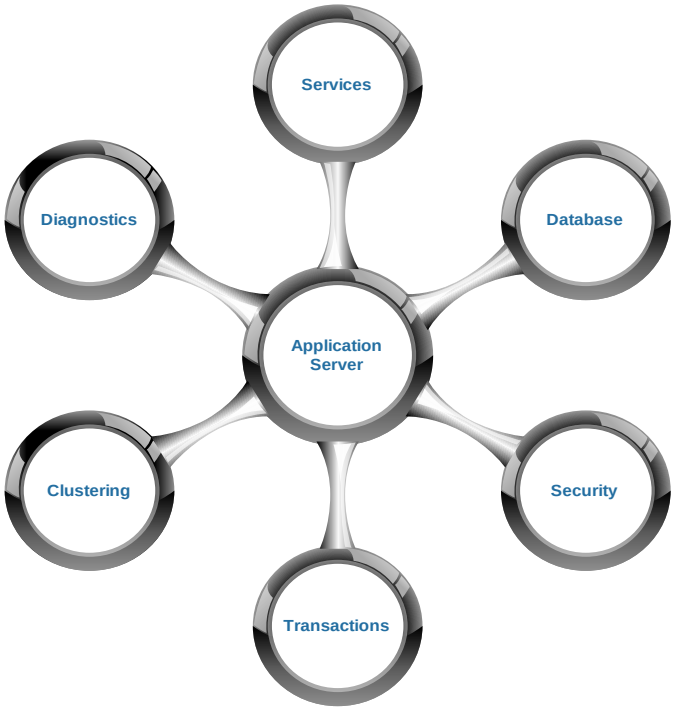

Fig. 2. Application Server functions

Fig. 2 shows the functions of the application server in a breakdown. The application server has a diagnostics attribute to track down and resolve errors. Security is a critical aspect in terms of trust management. This is to make sure malicious nodes to not end derailing the performance of the entire network. In the context of this paper, trust among nodes is compromised when one node withholds packets for a long time since transmission is through hops from one node to the other. Another active functionality of the application server is clustering. Clustering ensures fault tolerance of the application server. That is, in the event of hardware failure or part of application failure, services will remain running for users. The application server has a set of common services and also a database for record-keeping of all the transactions or rather.

b)Internet network provider: It is important to note the importance of the Internet Service provider (ISP) when evaluating the quality of experience(QoE). Operations taking place at this level of abstraction is not visible to the end-user.

The ISP plays a major role because in between application and web level, there has to be internet connectivity.

c)Web server: The web server plays an important role in the realization of HTTP web pages and connectivity. This technology is mostly on the user interface side. One can argue that it may be used in the evaluation of QoE. The browser is the main driving force behind the realization of the application stream. Basically, the browser translates these HTTP pages into media content e.g video, voice and FTP. Some web servers are found in the application server but this is not common in most application servers.

c)Operational chain: This shows the level of abstraction at which the framework is under. The user interface is where the end-user can manipulate the system and view the entire flow. The network level, however, is hidden from the end-user. The programmer or rather network specialist can, however, evaluate the performance of the system at this level. Our framework is evaluated from the application interface since we are not mainly interested in the experiences of the user but rather of the application itself in terms of performance.

d)QoS evaluation: QoS is the end-attainment goal of this trust framework and the framework encapsulates such an option. The evaluation of QoS or rather the provision of high QoS is what rates our framework. Different network detriments are observed while the system executes due to topology variations. QoS metrics like throughput, jitter, and delay and received routing packets. The end-user cannot determine the QoS of the system because it is at a different abstraction. The QoS results are a true reflection of the trust that exists among entities in the network. If the quality of service is poor, that would mean that the trust as well among nodes is poor.

e) *Direct trust*: Direct trust is application-centric which decides whether an interaction made between one entity and another was successful. Direct trust was chosen based on the merits that it is reliable in terms of rankings from confidence trust and reputation [20]. The framework operates from the point of view that the involved nodes do not necessarily need to have direct experience with all nodes in the network for them to be able to compute a particular trust level about them. In contrast, the trust is based on second-hand evidence that is provided by intermediate nodes. In this way, they benefit from the experiences of other nodes in the network. The framework designed is based on trust from interaction experiences. The attainment of good QoS in the network is evidence that the network itself is trustworthy. Good QoS in a dynamic topology network means or rather validates the framework. The direct trust can be computed using the formula:

$$\textit{Direct trust} = (g + (x)/2) / (q + x) \quad (1)$$

where **g** is the time success to say an event happened, **x** is a positive real number, and **q** represents the event transactions. If the first event of the transaction is a success, the direct trust value increases but inverse to this it decreases. In the trust framework, the success rate can also be referred to as the trust value and can be any real number between 0 and +1. In terms of QoS, the metric called delay plays a major role in finding the true trustworthiness of the network. This would mean that a specific node delivers packets on time and thus increased network efficiency. The trust being evaluated is from node to node

The parent architecture (figure 1) encompasses the concept of direct trust within an application server. Figure 2 depicts the relation and figure 3 fully shows the interaction in each node. The concept of MANET is exhibited through that each node works around its server. There is no centralized mechanism that controls activity and performance. As mentioned earlier, the idea of MANETs revolves around the idea that they are self-configuring and fig 2 shows the interaction of the application with direct trust. We assume that the application protects itself from malicious conditions. Here are a few definitions of concepts;

f) Trust Record: This component reveals information on the trust relationship between the application and the node. It also gives information on trust values in terms of their collection and storage.

g) Trust Computation: This component computes the trust value of the relationship between two different nodes. This computation can either give a 1(success) or 0(failure). The assumption is that

direct trust is based on the observation of activities performed by the application. This interaction happens in the application interface and is abstracted to the user. Relation 1 is either 1 or 0,Relation 2 is a 1 or 0, Relation 3 is either a 1 or 0 and Relation *n* is either a 1 or 0 too.

Fig 3 Application-based Direct Trust within a node

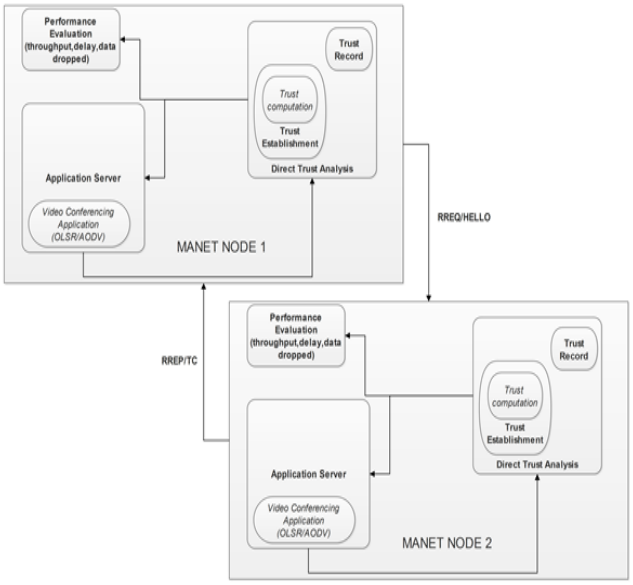

Fig 4 Node to Node Direct Trust

Fig 4 shows node to node interaction of either AODV/OLSR video conferencing traffic. It is important to note that MANET stations do not have a central controller and that is why every station has its application server. Every station is responsible for its application. Performance evaluation can be done at the node level and network level. The direct trust analysis depends on the interaction behavior of nodes together with their direct trust computation. After analysis, QoS performance evaluation can be conducted. The absence of a central controller gives each node the independence to execute functions remotely.

To fully understand the true meaning of trust, definitions of trust as adopted from social science must be firstly derived. Since this phenomenon is adopted from social science, there is no definite or precise definition in computer networks. It is often interpreted as reputation, trust opinion or even probability. The evaluation, as well, is done in many different ways using various models. Some models or rather schemes use continuous or discrete numerical values to quantify the level of trustworthiness. These are called quantitative trust models. There are many available trust models but it is still not clear as to the fundamental rules they must adhere to. This means that the design of these models is at an empirical stage. In the proposed framework (figure1), trust is viewed as intentional and that is, one node is willing to depend on another node. Trust intention brings out other concepts or constructs. The application remains in control of determining trust.

7. PROPOSED TRUST FRAMEWORK OPERATIONS

MANET communication plays a major role in the attainment of a proper flow of packets within the framework. Firstly, video packets will always move from the sender to the receiving end. The framework vividly shows two different interfaces that are involved, mainly the graphical user interface and application interface. The application interface can be abstracted as where the source of the video lies. It should also be noted that so much of bi-communication is involved around the different component parts. Before an application

can be sent, the application server as the middleware in this context has to ensure that direct trust is established. This means that the node has to be inspected in terms of its trustworthiness to service delivery. The application server is responsible for many functions including a database, clustering and as shown in Fig. 2. When the video file is sent through at the network level through the assistance of the Internet service provider, it is meant to reach the webserver. At this point in time, the video file is at the user interface side. The web server receives it as an HTTP file or page and translates it back into media content (video file). The webserver houses the web browsers just like application servers houses applications. Users get to stream the media content. The connection amongst these components remains bi-directional since trust must be maintained. QoS evaluation metrics like throughput, total packets dropped and Delay is implemented. Delay is an important QoS feature since it shows if there were selfish nodes or not. Evaluation can be done from the application interface (for QoS). The application interface and the user interface are both utilized the evaluation for QoE.

7.1 Experimentation

In this work, a high-level event-based network level simulation software called Optimized Network Engineering Tools (OPNET) was chosen. It is widely known for providing viable solutions towards performance analysis for networks and also applications. These simulations were carried out on a Windows 7.0 Professional Operating system (Desktop) with 3.40 GHz processor speed, 4.00 GB RAM and 64-bit Operating System. The set parameters are shown in Table 1:

Parameters	**Values**
Simulator	OPNET 14.5 Modeler
Protocols studied	AODV and OLSR
Simulation Area	1000*1000 meters
Simulation Time	900seconds
Node movement model	Random Waypoint
Transmission range	300m
Traffic type	Video Conferencing-High Resolution
Transmission Rate	11Mbit/s
File size	1024 bytes
Type of Service in QoS	Streaming Multimedia
Trajectory	Random
Transport Protocol Used	UDP
Speed	30km/h

Table 1 Set parameters

The scenarios of different protocol utilization were first analyzed and compared. The two routing protocols being analyzed and compared were AODV and OLSR. Each protocol has three different scenarios per QoS metric. The metrics in question are throughput, delay and data dropped. This meant twelve scenarios in total. Node scenarios had a total of 20 and 80 nodes respectively. All the simulations conducted are done in 4 hours.

7.1.1 20 Node-Scenarios

a) Throughput

Figure 5 shows the throughputs for AODV and OLSR. The Y-AXIS shows the throughput in bits/sec and X-AXIS shows time in hours and minutes. The first 3 minutes shows a positive hike up to 920 bits/sec in throughput and then a steady drop after 25 minutes of simulation time. A further drop is observed for the remaining simulation until it reaches 100bits/sec. OLSR, on the other hand, shows a major drop from 12 bits/sec to 5 bits/sec in the first 15 minutes of simulation. After 20 minutes, it picks up reaching an average of 8 bits/sec to 9.5 bits/sec for the remainder of the simulation even though it is still a poor throughput. This means that on an overall scale, AODV has a better throughput than OLSR.

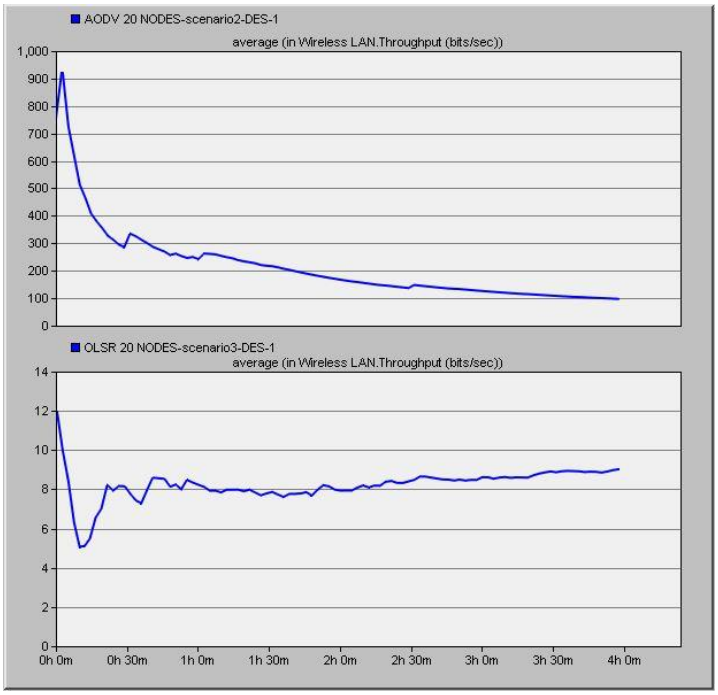

Figure 5 Average Throughput in bits/sec

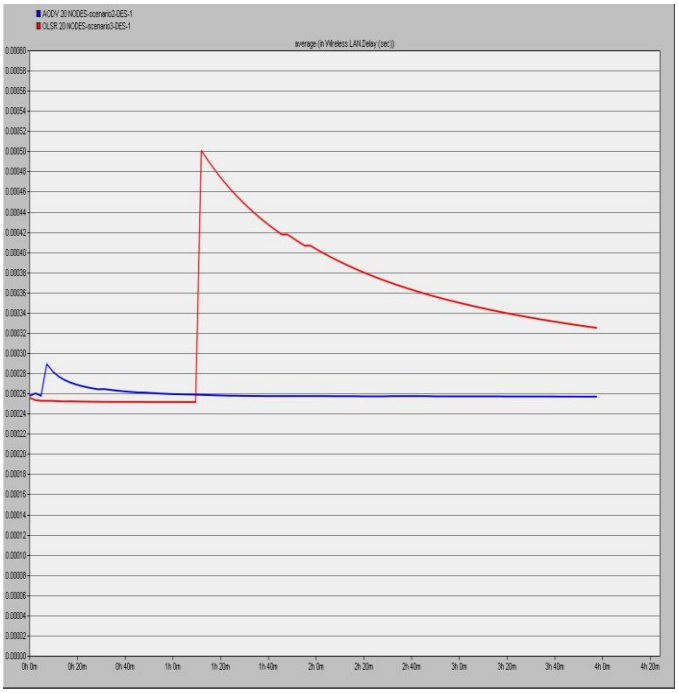

Figure 6 Network delay in sec

b) Delay

Figure 6 shows the network delay for AODV and OLSR protocols. In the first five minutes, AODV shows a slight rise in delay from 0.00026 bits/sec to 0.00029 bits/sec. This may be regarded as an insignificant rise in the eyes of the user but significant in terms of network efficiency. The delay drops again exactly after 5minutes back to a steady delay of 0.00026bits/sec. OLSR shows a constant delay of 0.00025bits/sec for the first 80 minutes of the simulation and then a sharp rise to 0.00050bits/sec after that showing a gradual drop to 0.00033bits/sec. In this scenario, OLSR has a significantly higher delay rate than AODV.

c) Data dropped

Figure 7, shows the average data dropped for both scenarios. The Y-AXIS shows the number of bits and the X-AXIS continues being our time represented in hours and minutes. OLSR shows a sharp rise for the first 3 minutes of simulation to 22 bits/sec then a sharp decline until about 20 minutes. The protocol further drops more data from the 18th minute until 20 minutes of simulation time. From there, the levels drop until they reach a margin of 4 bits/sec in data dropped on the 50th minute. It further grows again until 2 hours of simulation time then gradually shows a decline data dropped until it reaches 2.8 bits/sec. AODV shows no data dropped. This determination was performed a couple of times but remained on 0 bits/sec throughout the simulation period. OLSR has a relatively higher fate of data dropped than AODV.

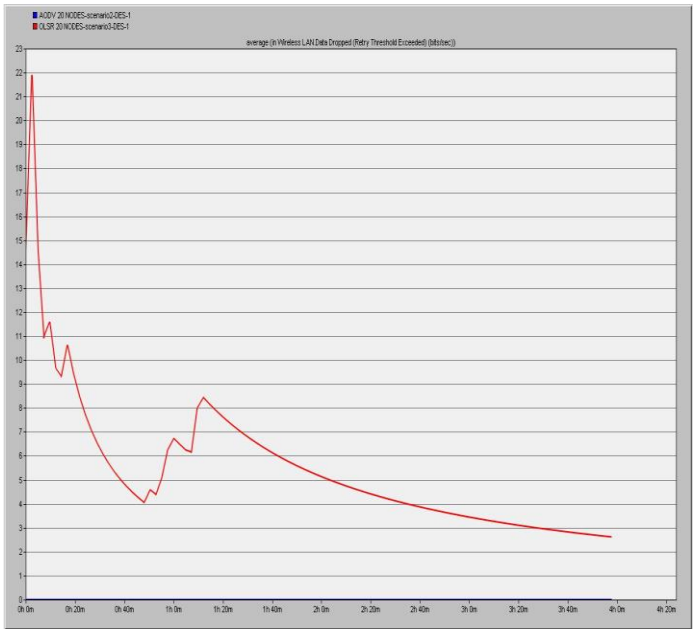

Figure 7 Average data dropped in bits per sec

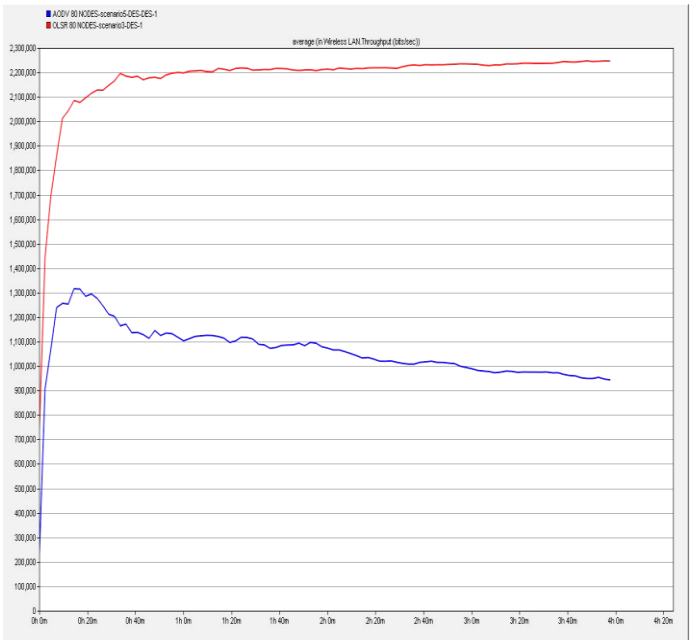

Figure 8 Throughput in bits/sec

7.1.2 80 Node-scenarios

a) Throughput

Figure 8 below shows the throughput of both ADOV and OLSR. The Y-axis of the figure shows bits/second and X-axis show time in hours and minutes. OLSR shows a continuous growth spiking up to an average peak of almost 2 200 000 bits/second and 800 000 bits/second being the lowest average throughput. After 15 minutes of simulation, the growth was then constant and steady until the end of the simulation. AODV showed an average peak throughput close to 1 300 000 bits/second after 15 minutes but overall it showed a spiking growth after the first 4 minutes of simulation from 300 000 bits/second to the latter. AODV, just unlike OLSR then dropped its throughput value until it reached 950,000 bits/second after 4 hours.

b) Delay

In figure 9 below, the delay exhibited steady and accelerated growth throughout the simulated time. The increase of the delay per second was sharp for both AODV and OLSR in the first 3 minutes of the simulation. The Y-axis shows a delay in seconds and X-axis show simulated time in hours and minutes. AODV showed an average peak delay of 0.040 seconds after 120 minutes of simulation and OLSR showed an average peak delay of 0.35 seconds. The delay is constant and not increasing after 20 minutes of simulation. AODV had a greater delay than OLSR.

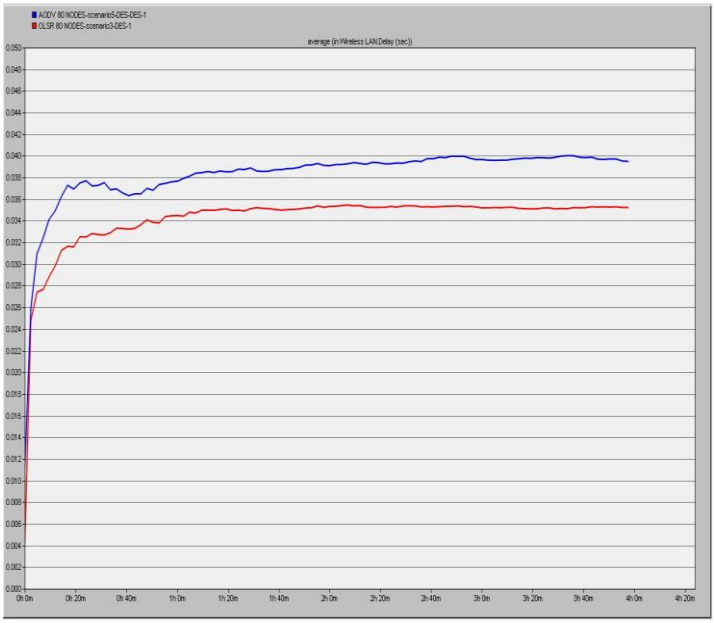

Figure 9 Delay in seconds

c) Data Dropped

In fig 10 below, the Y-axis showed data dropped in bits/second and the X-axis shows simulated time in hours and minutes. Both protocols have sharp rising data dropped increasing during the 18 minutes of simulation. AODV then dropped over time from an average peak of 245 000 bits/second to180 000 bits/second. OLSR showed an average peak routing traffic reception of about 240 000 bits/second after 2 hours of the simulation. Most of the growth happens in the first 20 minutes of simulation. Unlike AODV, OLSR does not decrease the amount of data dropped and thus making AODV better than OLSR in this scenario.

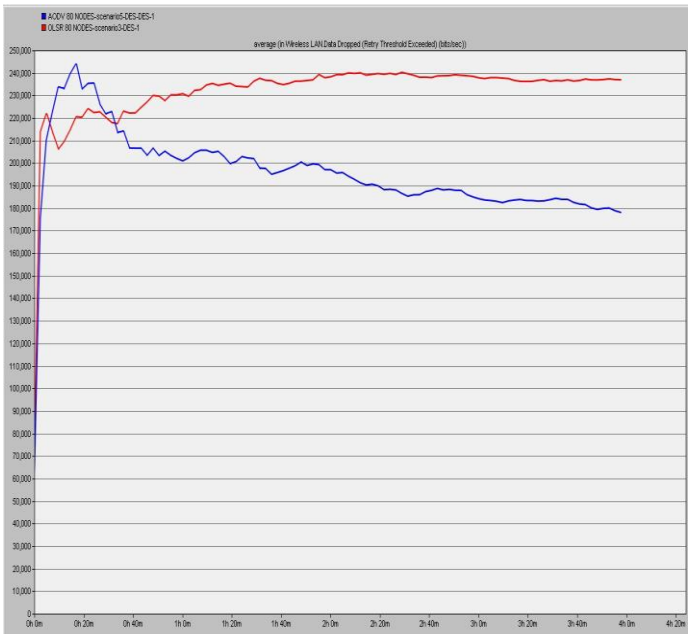

Figure 10 Data dropped in bits per second

8. CONCLUSIONS

This work presented and discussed trust management from the perspective of QoS in MANETs and proposed a trust framework called application-centric trust management framework with distributed trust computations (AppTrusFram) was presented and discussed. The essence is to ensure that nodes are trusted throughout their communication to ensure QoS delivery. The architecture of the trust framework was presented and provided an explanation of its components and operations. Based on its intended operations, we believed that if adopted for use in the realm of MANETs, it could go a long way to enhance the QoS delivery of video streaming. As future work, the utmost intention is to implement and evaluate the proposed framework as well as exploring other different trust establishment methods other than direct trust such as recommendation-based or even hybrid methods and so on.

Furthermore in this paper, an interaction of two nodes in transmission was presented. The framework addressed the type of trust utilized. The results obtained were very critical in terms of decision making of whether a particular protocol could be further developed to attain trust as well as the quality of service in the network. AODV and OLSR have great potential in terms of development to usable video streaming protocols. We analyzed, discussed and gave a comparison to results obtained. The results obtained are very critical in terms of decision making of whether a particular protocol could be further developed to attain trust as well as the quality of service in the network. The challenge that remains is within the tool OPNET 14.5 simulator, which limited the study in terms of an inability to provide specific measures in certain protocols and thus limiting us to choose statistics that would be globally analyzed, discussed and compared. For example, OLSR does not provide the measure of total packets dropped but rather packets dropped for individual nodes and this limitation makes it difficult to show those statistics since 80 mobile nodes would require 80 results graphs.

The measures used in this study, however, provided enough results to validate some parts of literature and to bring new findings in terms of quality of service and video streaming applications over MANETs. This evaluation is part of the framework proposed in terms of the application (video conferencing). The results also proved without any doubt that in terms of delay, these protocols perform well. Most of the scenarios had an average delay below the margin of one (1) second which is regarded as high response time in terms of network efficiency. The results obtained are very critical in terms of decision making of whether a particular protocol could be further developed to attain trust as well as the quality of service in the network. This evaluation is part of the framework proposed in terms of the application (video conferencing). The results also proved without any doubt that in terms of delay, these protocols perform well. Most of the scenarios had an average delay below the margin of one (1) second which is regarded as high response time in terms of network efficiency

9. ACKNOWLEDGMENTS

This work was supported by the FRC at the NWU-Mafikeng. We express our sincere gratitude and thanks to them as well as our colleagues in the Computer Science department.

10. REFERENCES

[1] S. Semplay, R. Sobti, and V. Mangat, "Review: Trust management in MANETs," *International Journal of Applied Engineering Research*, vol. 7, p. 2012.

[2] D. S. Aarti, "Tyagi, “Study Of Manet: Characteristics, challenges, application and security attacks”," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, pp. 252-257, 2013.

[3] A. Rajaram and D. S. Palaniswami, "A trust-based cross layer security protocol for mobile Ad hoc networks," *arXiv preprint arXiv:0911.0503*, 2009.

[4] P. Goyal, V. Parmar, and R. Rishi, "Manet: vulnerabilities, challenges, attacks, application," *IJCEM International Journal of Computational Engineering & Management*, vol. 11, pp. 32-37, 2011.

[5] M. S. I. M. A. Riaz and M. Tariqu, "Performance analysis of the Routing protocols for video Streaming over mobile ad hoc Networks," *International Journal of Computer Networks & Communications*, vol. 4, pp. 133-150, 2012.

[6] G. D. Delgado, V. C. Frías, and M. A. Igartua, "Video-streaming transmission with qos over cross-layered ad hoc networks," in *2006 International Conference on Software in Telecommunications and Computer Networks*, 2006, pp. 102-106.

[7] M. Lindeberg, S. Kristiansen, T. Plagemann, and V. Goebel, "Challenges and techniques for video streaming over mobile ad hoc networks," *Multimedia Systems*, vol. 17, pp. 51-82, 2011.

[8] Y. Singh and M. V. Siwach, "Quality of Service in MANET," *Int. J. Innov. Eng. Technol*, 2012.

[9] N. Sharma, S. Rana, and R. Sharma, "Provisioning of Quality of Service in MANETs

performance analysis & comparison (AODV and DSR)," in *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on*, 2010, pp. V7-243-V7-248.

[10] J. Sen, "A survey on reputation and trust-based systems for wireless communication networks," *arXiv preprint arXiv:1012.2529*, 2010.

[11] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," *IEEE Communications Magazine*, vol. 46, pp. 108-114, 2008.

[12] R. Ferdous, V. Muthukkumarasamy, and A. Sattar, "Trust Management Scheme for Mobile Ad-Hoc Networks," in *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 2010, pp. 896-901.

[13] I. Ahmad, H. Jabeen, and F. Riaz, "Improved quality of service protocol for real time traffic in manet," *arXiv preprint arXiv:1308.2797*, 2013.

[14] M. Rao and N. Singh, "Quality of service enhancement in MANETs with an efficient routing algorithm," in *Advance Computing Conference (IACC), 2014 IEEE International*, 2014, pp. 381-384.

[15] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 14, pp. 279-298, 2012.

[16] V. Singh and M. Jain, "Secure AODV Routing Protocols Based on Concept of Trust in MANET's," *topology*, vol. 3, 2014.

[17] J. Sen, "A distributed trust management framework for detecting malicious packet dropping nodes in a mobile ad hoc network," *arXiv preprint arXiv:1010.5176*, 2010.

[18] N. Li and S. K. Das, "A trust-based framework for data forwarding in opportunistic networks," *Ad Hoc Networks*, vol. 11, pp. 1497-1509, 2013.

[19] X. M. Zhang, Y. Zhang, F. Yan, and A. V. Vasilakos, "Interference-based topology control algorithm for delay-constrained mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 14, pp. 742-754, 2015.

[20] R. Kiefhaber, R. Jahr, N. Msadek, and T. Ungerer, "Ranking of direct trust, confidence, and reputation in an abstract system with unreliable components," in *Ubiquitous Intelligence and Computing, 2013 IEEE 10th International Conference on and 10th International Conference on Autonomic and Trusted Computing (UIC/ATC)*, 2013, pp. 388-395.

[21] T. Phakathi, F. Lugayizi, B. Isong and N. Gasela, "Quality of Service of Video Streaming in Vehicular Adhoc Networks: Performance Analysis," *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, 2016, pp. 886-891.

[22] A. Chen, G. Xu, and Y. Yang, “A Cluster-Based Trust Model for Mobile Ad Hoc Networks,” 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing, 2008