Reducing Security Vulnerabilities in Software Defined Mobile Network

A. Venugopal
Assistant Professor, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India.

Anila. N. V
M.Phil Scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore, Tamil Nadu, India.

Abstract – Mobile networks are increasing drastically with different types of applications and features. This reliable feature and creates various types of attacks in the computer network. Software Defined Mobile Network (SDMN) is the new approach to the mobile networks to adopt all features and that can be implemented in software. This software's are referred with the protocols to deploy the complete network architecture. Due to this scalable and reliable character, the SDMN is affected by the DoS and spoofing related attacks. To prevent and detect the attacks in SDMN, different types of research ideas are deployed in this proposal. The system aim to reduce the security threats on the SDMN by deploying a new program in the routing protocol named as secure Software Defined Mobile Network Routing Protocol (SSDMNRP). This deployed to limit the flow acceptance to verifiable sources, to tackle the problem of unwanted traffic, source address spoofing, and thus prevent resource exhaustion. To eliminate source address spoofing, proposed protocol used MAC (Message authentication code) technique. This also avoids node misbehaves in the network and application layers of SDMN. To perform trust routing, the system aggregates misbehavior evidences and calculates the trust score for every node, and contribute towards using reputation mechanisms for improving the security of communicating entities. So a stable reputation system has been developed. The verification of nodes allows defining dynamic MAC keys for nodes to perform and track services. The implementation has performed in NS2 and the experiments are shown that the proposed system performs better security in the SDMN architecture well than the existing system.

Index Terms – Mobile Network, Security, SDMN, Message authentication code, Network attacks.

1. INTRODUCTION

In the recent scenario software defined network is emerged tremendously. A Secure SDMN is a developing technology that is finding activity in the field of network safety and administration [1]. The Secure SDMNs have benefits like overcome network latency, dropping network load, executing asynchronously and autonomously, adapting dynamically, operating in heterogeneous environments, and having tough and fault-tolerant performance when put side by side with other systems [2]. As stated Secure SDMNs are helpful in network safety, this can use variety of Secure SDMNs for protect the network from the threats [3], also this can identify the threats, for example network sniffing detector in Secure SDMN used to discover the network sniffer computer in the network. SDMN is a rising technology that makes it a lot easier to design, apply, and maintain extend systems remotely. SDMNs are programs that can be send out from one computer and transfer to a remote computer for execution. They resolve the problem in the client/server network bandwidth by creating an agent to handle the doubt and sending it to where the data exist in rather than passing link outcome and information over the wire. Agents decrease design risk since decisions such as the location of program can be pushed toward the end of the development and the system can be easily modified after it is built and in operation. This kind of architectures also can solve the problems on the basis of untrustworthy network connections, which suit the mobile device atmosphere where the devices cannot always connect to the network. In the past few years, a lot of Secure SDMN systems [4][5] have been developed. These systems, all meet the basic necessity of the capacity to transfer the state of an agent and to continue its execution on the destination host. However, their design approaches are different.

In few years, intrusion and other types of attacks to the software defined computer network systems have become more and more extensive and sophisticated. In addition to intrusion prevention techniques [6] such as authentication, firewall and cryptography used as a first line of defense, intrusion detection is often used as a second line of defense to protect computer networks. Intrusion detection is defined as the problem of identifying individuals who are using a computer system without authorization and those who have legal access to the system but are abusing their rights (i.e. Man in Middle) Secure SDMNs are programs with persistent identity, which move around a network on their own decision and can correspond with their environment and with other agents. These systems use specific servers to interpret the agent's behavior and correspond with other servers. So there is a necessary to deploy a complete security for SDMN. In order to overcome many of the limitations of existing security SDMN [7], simulation tool is used and developed to show the benefits of using Secure SDMNs to perform security. Secure SDMNs' ability to

autonomously mange the whole network with the single software based solution embedded with the routing protocol. Their ability to travel through the network and carry data along with them enables the agents to hide data, code, and security-relevant information from potential attackers. The followings are the proposed system research objectives.

1. Aim to support network by providing cost-effective solution.
2. Aim to monitor the system to perform security and prevention from vulnerable attack.
3. Aim to maintain the network security and to detect the DoS attacks in SDMN.
4. Aim to provide the security features with the trust calculation.
5. Aim to avoid unauthorized access in the mobile network and mitigate the different types of attacks like Spoofing, DoS and unauthorized node access.

Moreover, the security of the network is not vulnerable to a single point of failure and the security can continue even if individual nodes fail or become unavailable. Here, proposed routing protocol can compute and append the signature on one host and travel to another host or set of hosts and report the results. The trust analysis enables the detection of attackers and routes on the secure path.

2. PROBLEM DEFINITION

Nowadays, various types of attacks (internal and external) to the computer network increasing day by day. Primarily the prevention methods of intrusion detection are used to protect computer networks. Secure SDMNs are with determined identity. Secure SDMNs are composition of computer software and data which migrates from one computer to another. While doing this, they continue their itinerary up to the home computer. Autonomy and mobility are main features of Secure SDMNs, specifically this is a more challenging where a mobile node moves from one environment to another environment, with remains data intact. Secure SDMN itself decides when and where to move. When a Secure SDMN decides to move then they save their own state and this state transport to another host. Secure SDMNs are specific about mobile code and they are choosing the host and also active in respect of execution. Secure SDMNs have special characteristics which can help intrusion detection in several ways. The use of security architecture in SDMNs computing paradigms have been proposed in several researches. The advantages include: overcoming network latency, reducing network load, executing asynchronously and autonomously, adapting dynamically, operating in heterogeneous environments, and having robust and fault-tolerant behavior. The existing SDMN architecture, security challenges and recent techniques on SDMN have discussed in the literature [8]. Form the analysis and interpretation, the proposed system have developed.

3. PROPOSED SYSTEM

3.1 INTRODUCTION:

Safe and secure message communication in Software Defined Mobile Network has become very important in today's network environment. Such messages that transmitted through intermediate nodes need to be validated based on their trust and reputations. Hence, this research work proposes a trust and reputation in network communication in Software Defined Mobile Networks. Source node transmits the message to destination node, the assistance of intermediate nodes are very important and they plays important role in forwarding the packets to appropriate destination node .The establishment of node cooperation and node reputation leads the successful packet delivery from the source node to destination node through intermediate nodes. This proposed work reveals the details of neighbor node discovery, the Secure nodes, trusted and reputed nodes to find and isolate the attacker nodes. The proposed system architecture for trusting the node and its reputation for secure communication in SDMN is shown in Figure 1.0. This proposed system architecture consists of various functionalities namely node discovery and identifying the node reputation.

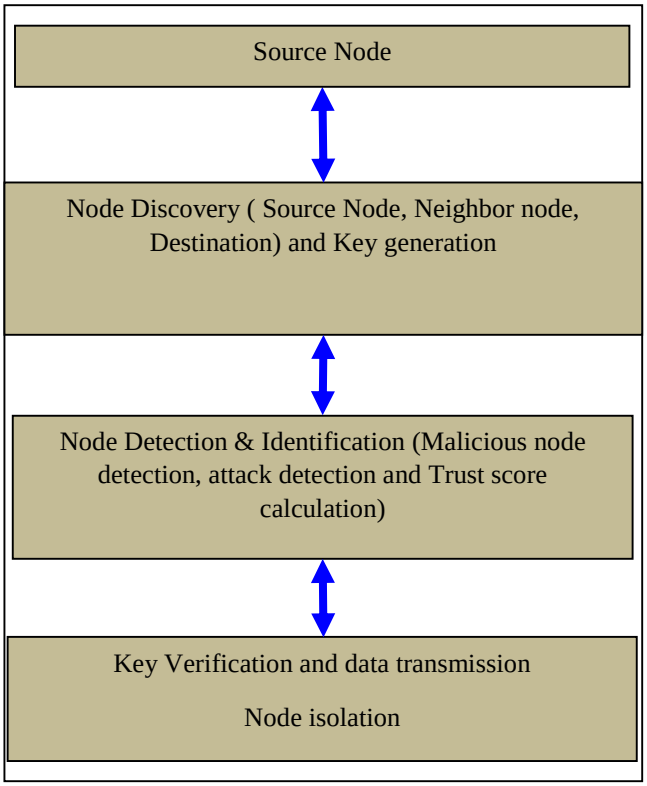

Figure 1.0System Architecture for Trusted and Reputed secure Communications in SDMN

The proposed system has different types of research contributions; the following provides the list of the contributions.

- The proposal aim to reduce the security threats on the SDMN by deploying a new program in the routing protocol named as secure Software Defined Mobile Network Routing Protocol (SSDMNRP). This deployed to limit the flow acceptance to verifiable sources, to tackle the problem of unwanted traffic, source address spoofing, and thus prevent resource exhaustion.
- To eliminate source address spoofing, proposed protocol used MAC (Message authentication code) technique to avoid node misbehaves.
- Make it possible to aggregate misbehavior evidences under a stable source identity, and contribute towards using reputation mechanisms for improving the security of communicating entities. So a stable reputation system has been developed.
- Under network stress, grant resources based on source trust score.
- Allow defining dynamic MAC keys for nodes to perform and track services.

This is in contrast to the current mobile networks where policies are tightly coupled to physical resources and are not scalable to services/applications.

3.2 SECURE NODE SELECTION:

3.2.1 Neighbour Node Discovery and Identification of Secure Nodes:

In software defined mobile networks, the discovery of neighbour node is must in order to find suitable neighbour nodes while there is a communication between the source node and destination node. Each node finds their neighbour nodes that are within the communication range in software defined mobile networks. For this, a HELLO message is passed to identify the neighbour Source Node Elimination Destination Co-operative node Source Node Malicious Neighbourhood Node Node Reputed node Destination node Attacker Node Bargaing for Agreement Price Fixing Agree Dis Agree Node Lifetime management Co-operative Route Establishment & Maintenance Forward Node List Updation Database Node Discovery Node Detection & Identification Bargain Process node trust and its reputation in SDMNs. In addition, the past history of message transmission is used to find the Secure and non-Secure nodes in software defined mobile networks.

3.2.2 Detection of Non-Secure Nodes:

The source node identifies the intermediate co-operative nodes for forwarding the packets to the destination node in SDMNs. There are several effective methodologies to identify the co-operative nodes in SDMN. From them the node rating algorithm is used to measure the identity of the packet delivery ratio, throughput of relay nodes and other factor while communication takes places. Moreover in software defined mobile networks, the transmission range of mobile nodes is limited due to the power constraint. Hence, communication between two nodes beyond the transmission range relies on intermediate nodes in order to forward the packets. But, sometimes these intermediate nodes do not properly respond due to its limited resources such as energy, bandwidth etc. Such nodes are assumed as non-Secure nodes or misbehaving nodes. The non-Secure nodes are classified as x Malicious Nodes x Attacker Nodes

3.2.2.1 Malicious Nodes:

The malicious nodes will always attempt to reduce the network connectivity and will pretend that they are Secure in nature. But, in fact all the packets are bypassed to non-directed node thereby delaying the packet delivery. Hence, several types of attacks are performed by malicious node such as Denial of Service (DoS) attack, Black hole attack, Wormhole attack and Rushing attack. These types of attacks lead to unnecessary route request control messages, and frequent generation of beacon packets or forwarding of stale information to nodes. Hence, these malicious node actions isolate the nodes and drastically reduce the network performance.

3.2.2.2 Attacker Nodes:

Attacker nodes are those which neglect the packets that are to be forwarded by them in mobile ad hoc environments. Usually attacker nodes will not cooperate in data transmission process which causes serious threats to network performance. Hence, the attacker nodes always try to reduce the performance in SDMNs. The attacker nodes are categorized into following facts. Fact I. The attacker nodes that participate in routing process but it will not forward the data packets that they have received. Hence, the packets may be dropped instead of being forwarded to its respective destination node. Fact II. The attacker nodes will not participate correctly in routing process thereby hiding available routes. For example, the attacker nodes may drop all Route Request that it receives and does not forwards a Route Reports to the destination in DSR.

3.3 LOCATION AIDED SECURE ROUTING SCHEME FOR SDMN:

To design an effective incentive scheme the location aided routing protocol is used in this research work. Location aided routing protocol observes the real process of the node which does not move around randomly but rather move in a predictable fashion based on mobility patterns. If a pair of nodes has met several times before, then it predicts the pair of nodes that will meet in future. This kind of mobility patterns are exploited to improve the performance of routing protocol

in software defined mobile networks. Also, the existing location aided routing protocols lack in incentive mechanism. Hence, an efficient incentive mechanism is needed for stimulating attacker nodes in order to forward the messages with higher delivery probability to reach the desired destination. This is achieved by two mechanisms namely bargaining based agreement/disagreement and attacker node elimination.

3.3.1 Key based Agreement and Disagreement:

To insist the concepts of incentive compatibility of location aided routing, the Key based packet forwarding scheme is applied in this research work. The messages that are valuated as lower delivery probability nodes will be selected in order to deliver or forward the messages communication with the higher delivery probability nodes. This is achieved by giving the security key at the time of transmission. The key table maintains all the accounts of the transactions. This process is carried out with required numbered of rounds until it reaches the agreement with sufficient nodes that are to be participated in the message communication.. This key generation and verification process is introduced carefully with the effective MAC algorithm called Chaskey algorithm. The main idea behind this routing scheme is to stimulate the attacker nodes to actively participate and forward the packets to its receiver node in the communication process.

3.3.2 Node Detection and Elimination:

The idea behind the node detection and elimination process is to establish the proper connectivity and enhance the Secure and reputed strategy in SDMNs. When the there is no incentive mechanism, then the attacker or misbehavior node is identified and isolated through the proper approach thereby providing secure message communication. 48 In addition with software defined mobile software defined mobile networks, the attacker nodes are made to simulate and induce the attacker node to participate actively in message communication process. Moreover, the bargaining process and an effective message trading scheme are applied to do this incentive mechanism for the participation of attacker nodes in communication. If the bargaining process is not charged between the nodes, then the attacker nodes are isolated from the network to ensuring the smooth and effective Secure communication.

3.4 SECURE ROUTE ESTABLISHMENT AND MAINTENANCE:

The Secure route establishment and maintenance is another major contribution in this research work. Apart from the attacker and misbehavior node identification, the identified Secure, trusted and reputed nodes are involved in establishing the proper route and maintenance for the safe and secure packet delivery. In Software Defined Mobile Networks, several efficient protocols are available such as Object Link State Routing (OLSR), Ad hoc On Demand Distance Vector (AODV), Dynamic Source Routing (DSR) and Secure Medium Access Control (CMAC). But in this contribution, OLSR, Enhanced Secure Software defined mobile Routing (ECOR) and Enhanced Distributed Energy Location based Secure Medium Access Control (EDEL-CMAC) are used in our implementation in order to establish the best Secure routes and for efficient energy savings. The two main contributions that represent the node selection and list updates, path identifications and path maintenance during the packet transmissions in secure communication are elaborated as follows.

3.4.1 Updating the List of Forwarding Nodes: The first contribution is that the identified secure nodes are updated in the knowledge base for secure packet transmission during communication in software defined mobile networks. Once the Secure nodes are identified by the relay nodes, the identified secure nodes are disseminated in the network for establishing the secure list update and reputed message communication via the secure relay nodes. This list of forwarding nodes are updated and maintained by all the nodes with the influence of available first hand and second hand information in the ad hoc networks.

3.4.2 Secure and Reputed Packet Delivery: The second contribution in this proposed research work is Secure and reputed packet delivery in Software Defined Mobile Networks. The route is established via the appropriate protocol with the Secure nodes which is maintained for the message communication or information delivery. This identified Secure route is utilized for the secure and safe transmission of message from source node to destination through the intermediate nodes.

3.5 ENERGY OPTIMIZATION IN SDMNS:

In software defined mobile networks, the nodes are operated in battery powered during communications. Hence, the energy consumption of mobile nodes is an important factor among the various factors that are considered in this research work. To perform various tasks in the network with the trust, and reputation based Secure communication, the energy plays an important role. Hence, the optimization of energy is more important for attaining the increased lifetime of the network. The effective relay selection algorithm and Network Vector Settings (NAV) are appropriately incorporated in this research work in order to reduce the energy consumption in SDMNs. This Network Vector setting optimizes the energy consumption which leads to effective communication which leads to effective delivery of the packets in software defined mobile networks.

4. RESULTS AND DISCUSSIONS

This research work was implemented using NS2 Network Simulation Tool. The simulation was carried out with a field size of 1500m x 300m with 50 numbers of nodes. In this

simulation, the nodes will move within the network space according to the random waypoint mobility model. In random waypoint mobility model and each node will move to a random location within the specified network area. Once node arrives at the target location, it remains for a pause time before it moves to another random location. The pause time will set to 0.5 second. The communication patterns will have Constant Bit Rate (CBR) connection with a data rate of 3 packets per second. 15 connections will establish at random so that each node would chance to connect to every other node. The various parameters used in this simulation were shown the Table 1.0.

Table 1.0 Simulation Parameters for Enhanced Trust SDMN Routing

Parameter	Value
Antenna	Omi antenna
MAC Protocol	802.11
Mobility Model	Random waypoint
Topology Area	1500mm×300mm
Number of Nodes	50
Transmission Range	250m
Packet Size	256b
Traffic Type	CBR
Simulation Duration	300s

The performance of secured trust communication was simulated using Network Simulator NS2 and the experiments were carried out for the proposed scheme and the resulting values were compared with the existing systems. The obtained values are plotted as line chart graphs for representing performance and comparative analysis. The comparison of packet dropping ratio between the proposed and existing protocols was made through the network simulations. Figure 2.0 shows that the proposed scheme is more trust and minimizes the packet loss in the networks.

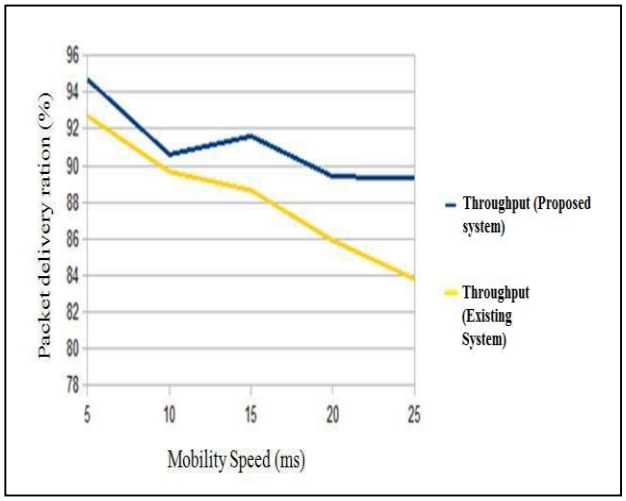

Figure 2.0 Performance Analyses between Throughput in SSDMNRP and existing protocol

The comparison of packet delivery ratio between the proposed and existing protocols was made through the network simulations. The proposed scheme represents the improvisation as well as the node trust in SDMNs. It is successfully simulated based on the primary and secondary rating among mobile nodes. This is achieved through the packet delivery ratio and throughput of relay nodes while the communication occurs in this network.

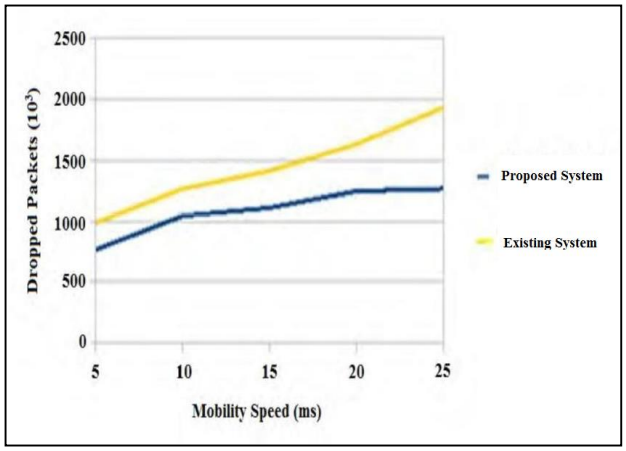

Figure 3.0 Comparison of Node Mobility with Packet Dropping Ratio among Existing protocols and SSDMNRP

The performance analysis between nodes' mobility with packet delivering ratio of SSDMNRP and existing protocols is shown in Figure 3.0 identifies the trust is achieved through higher PDR ratio and the relay nodes are identified their neighbor nodes. The proper routes are calculated and established based on the rewarding the mobile nodes in a network. The maximum throughput is achieved using SSDMNRP and it leads trust transmission by elimination of nodes' lower rating ratio and the reputation among the network is also achieved.

5. CONCLUSION

This paper investigated the security vulnerabilities in SDMN (Software Defined Mobile Networks) and proposed novel security architectures to mitigate them. In this proposed work, the reputed and node communication is achieved using different efficient schemes. Also various matrices such as packet delivery ratio, packet dropping ratio, packet transmission delay, throughput, uncertainty reduction and selfish node participation are utilized to attain the reputation based secure data packet transmission in the SDMN. The issues behind the nodes' lifetime are concentrated with this work, when there is a cooperative packet delivery SSDMNRP with new algorithm. The network allocation vector settings are perfectly handled and it is used in a large scale SDMN for energy savings and secure communication. Thus the entire network life time is also achieved simultaneously when the reputed node communication in software defined mobile networks.

REFERENCES

[1] Hu, Fei, Qi Hao, and Ke Bao. "A survey on software-defined network and openflow: From concept to implementation." *IEEE Communications Surveys & Tutorials* 16.4 (2014): 2181-2206.

[2] Chen, Tao, Marja Matinmikko, Xianfu Chen, Xuan Zhou, and Petri Ahokangas. "Software defined mobile networks: concept, survey, and research directions." *IEEE Communications Magazine* 53, no. 11 (2015): 126-133.

[3] Chen, Min, Yongfeng Qian, Shiwen Mao, Wan Tang, and Ximin Yang. "Software-defined mobile networks security." *Mobile Networks and Applications* 21, no. 5 (2016): 729-743.

[4] Liyanage, Madhusanka, An Braeken, Anca Delia Jurcut, Mika Ylianttila, and Andrei Gurtov. "Secure communication channel architecture for Software Defined Mobile Networks." *Computer Networks* 114 (2017): 32-50.

[5] Liyanage, Madhusanka, Ijaz Ahmad, Jude Okwuibe, Mika Ylianttila, Hammad Kabir, Jesus Llorente Santos, Raimo Kantola, Oscar Lopez Perez, Mikel Uriarte Itzazelaia, and Edgardo Montes de Oca. "Enhancing Security of Software Defined Mobile Networks." *IEEE Access* (2017).

[6] Resmi, A. M., and R. Manicka Chezian. "An extension of intrusion prevention, detection and response system for secure content delivery networks." *Advances in Computer Applications (ICACA), IEEE International Conference on*. IEEE, 2016.

[7] Liyanage, Madhusanka, Ahmed Bux Abro, Mika Ylianttila, and Andrei Gurtov. "Opportunities and challenges of software-defined mobile networks in network security." *IEEE Security & Privacy* 14, no. 4 (2016): 34-44.

[8] A.Venugopal, Anila. N. V. "Security Analysis on Software Defined Mobile." *International Journal of Advanced Research in Computer and Communication Engineering*, 2017: 109-113.