Circuits and Systems, 2016, 7, 239-254
Published Online April 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.74023

Scientific Research Publishing

Secured Efficient Fast Handover Multihoming Based NEMO+ (SEFMNEMO+) for Vanets

M. Siva Sangari[1], K. Baskaran[2]

[1]Information and Communication Engineering, Anna University, Chennai, India
[2]Department of EEE, Government College of Technology, Coimbatore, India
Email: ssangari.cbe@gmail.com, drbaskaran@gct.ac.in

Received 21 February 2016; accepted 18 April 2016; published 21 April 2016

Abstract

Vehicular Ad Hoc Network (VANET) is an emerging technology in which mobility management, continuous connectivity and security on data transmission between vehicles with high speed or during the change of topology of the network acts as a challenging exploration issue of Intelligent Transportation System (ITS) applications. This paper aims to formulate a ubiquitous connectivity to nodes by keeping the established connections before and after handover thereby minimizing the delay, packet loss and provide secured acknowledgement for handover. The Secured Efficient Fast Handover Multihoming Based NEMO+ (SEFMNEMO+) framework helps to optimize the NEMO+ scheme that supports multihomed network, handover and security. The predictive policy exchange method is used to update the future handover for minimizing the overhead delay and packet loss. The multihomed feature in NEMO+ supports efficient handover mechanism between heterogeneous networks when VANET connection fails. Public key cryptography provides the secure acknowledgement before handover *i.e.*, the acknowledgement is encrypted with digital signature.

Keywords

VANET, Intelligent Transport System (ITS), Multihoming, Handover

1. Introduction

Vehicular network adapts the techniques of Intelligent Transportation Systems (ITS) [1] that provide telematics services to avoid collision [2] [3] exclusively based on vehicle sensors. Safety services are the most important in ITS solutions, because vehicular networks are commonly used to exchange navigation and road-side events with

How to cite this paper: Sangari, M.S. and Baskaran, K. (2016) Secured Efficient Fast Handover Multihoming Based NEMO+ (SEFMNEMO+) for Vanets. *Circuits and Systems*, **7**, 239-254. http://dx.doi.org/10.4236/cs.2016.74023

the aim to prevent from potential hazards. Nonetheless, comfort, traffic management and monitoring systems, other services like vehicle tracking, parking reservation, platooning, and distributed games also depend on vehicular networks. Several communication paradigms is involved in vehicular networks, such as vehicle to vehicle (V-V), infrastructure to vehicle (I-V), vehicle to infrastructure (V-I), and infrastructure to infrastructure (I-I).

VANET [4] or Vehicular Ad-hoc Networks [5] is implemented in ITS based on the strategy of communication paradigms. IP mobility solutions [6] and VANET routing protocols [7] [8] are combined for communicating the vehicles. IP mobility solutions are accepted widely and it provides the nodes to access the reachability of global Internet [9] and session continuity. Among highly-mobile vehicles, in a fully distributed manner, VANET routing protocols provide wireless multi hop communication [10] [11] in working group of Network Mobility (NEMO) [12].

NEMO is aligned with Mobile IPv6 [13], where NEMO BS needs IPv6 [14] mobility for entire moving networks and it reduces the signaling overhead by Handovers through Mobile Router, and it shields the nodes movements in the mobile network and thus enables the device usage that are not provided with NEMO BS and the connectivity for mobile network nodes (MNNs) are provided by the MR. In MIPv6, it inherits the loss of packet and long handover latency during the handover. In NEMO, as MNNs move in a mobile network [15], at the same time these issues become more critical. These problems [16] [17] are overwhelmed by the mobility that support with a standard IPv6 protocol.

In this paper the EFNEMO+ [18] uses trinity protocols such as Tree Discovery, NINA and RRH. The best part is that the protocols are used to route the packets efficiently in efficient fast handover NEMO+ mechanism which eliminates the burden of burrow between PAR and NAR. EFNEMO+ adopts the tentative binding update (TBU) scheme [19] [20] to register a new care-of address (NCoA) with the MR's home agent (HA) early. Then, these packets are destined by MNNs that are delivered via various paths between the HA and the NAR. As the registration to the HA is performed in advance thus burrowing is not used in EFNEMO+ and the handover latency is reduced. However the BU message is still vulnerable to attacks such as: the Man-In-The-Middle (MITM) attack, session hijacking attack, Denial-of-Service (DoS) attack. To avoid from those attacks, the BU message encrypted and signed using the Private Key-based Binding Update (PKBU) protocol [21] [22].

Tarik Taleb *et al*. [23] presents to reduce the traffic globally in VANET networks and to minimize the inundations during links that are created for selected paths. Routing using by receiving on most stable group-path (ROMSGP) scheme is introduced to prevent the broadcast gales that arise during the path discovery operation.

D. Tamil Selvan *et al.* [24] present prediction based packet transmit at the intersection zone to avoid packet loss and usage of bandwidth while rebroadcasting. The two predictions are node prediction and mobility prediction to deliver the Packet or data in the network. At the intersection zone the prediction can be used successful delivery of data then the Bandwidth usage is less and decreased Bandwidth.

Dae Won Lee [25] says that the characteristics of vehicles' mobility are analyzed with the navigation information; then it the mobility is classified into intra highway mobility and global mobility management. Furthermore, mobility management scheme based on route prediction in VANET are implemented for Handoffs with intra highway mobility.

Park, Hee-Dong, *et al*. [26] say that the seamless handover scheme in multihoming using a mobile router with dual egress interfaces for wireless train networks. The scheme organizes twin antennas that are located at each end of the train for space diversity and each egress interface of a mobile router are get connected together. In mobile router, one of the two egress interfaces through its antenna it continuously receive packets while the other is undergoing a handover, that provides no service disruption or packet loss.

Illkyun, *et al.* [27] says that code calculation and cost delay of authentication are reduce by implementing SK-L^2-AM (Symmetric Key Based Local-Lighted Authenticated mechanism) and piggyback method is implemented in AX-FPMIPV6 (Authentication Extension of Fast Handoff for PMIPV6) to reduce the overhead of authentication and signaling to provide better handoff and authentication.

2. Proposed Methodology

As a part of the analysis done on Vehicular handovers, the following methodology namely Secured Efficient Fast Handover Multihoming Based NEMO+ (SEFMNEMO+) is proposed.

In SEFMNEMO+, the registration of MR to HA be performed in advance to enhance the handover progression,

i.e. an uncertain registration to HA is done simultaneously before actual handover is happened. Mobile Network Nodes (MNN) conveys the packets between MR and NAR in different path, but not through the burrow between PAR and NAR in order to diminish the burden in the burrow and idleness of handover. The optimize delivery of the packet to the destination network is performed using the triad protocol such as Tree Discovery (TD), Network In Node Advertisement (NINA), Reverse Route Header (RRH). SEFMNEMO+ mechanism is introduced in multi homed mobility configuration based on flow binding to access the destination network from multiple network to predicts the handover process by accessing the information about actual location and previously recorded context data. In order to provide the seamless connectivity to the MR the predictive policy exchange message is used and it will avoid packet from the delay and loss during handover. The Private Key-based Binding Update (PKBU) protocol is to effectively protect the FBU message against attacks by adversary.

2.1. NEMO+ Scheme with Efficient Fast Handover (EFNEMO+)

EFNEMO+ scheme is used to optimize the delivery of packet in the VANET. The optimize path is decided using interoperation protocols such as

- Tree Discovery (TD) is used to describes the flows of message out of MR Ingress interface
- Network in Node Advertisement (NINA) is used to subsequent flow of message out of MR egress interface.
- Reverse Route Header (RRH) is used to establish the registrations of MR in HA.

NEMO+ efficient handover mechanism is introduced in multihomed mobility configuration based on flow binding to access the destination network from multiple networks. It predicts the handover by using the actual location information and previously recorded context data.

2.2. Connecting Multiple MR Using TD

The first level of protocol in NEMO+ is Tree decision (TD) protocol which is used to discover and connect multiple MR in the network. With IPv6 Neighbor discovery (ND) Route Advertisement (RA) augments it by MR to transmit the TD, which allows MR to distribute information among the other MR that connects to its ingress interface. This helps MR to decide which MR has to connect with other MR in order to form a tree structure. This is achieved by Tree Information Option (TIO) which is augmented in RA as RA+TIO, where TIO has the information regarding the TD that decides the MR whether to connect another MR or not. Spontaneous attachment of MR will be designed as graphs by itself which do not accept to form loops, because looping may conflicts the MR when it is listening to RA from its own Ingress interface to access the internet. The aim of TD is to prevent router from looping. This is achieved through TD that provides the information regarding the router selection and it carries another information such as whether MR in the tree is connected to internet, or how long each MR in the EFNEMO, or the bandwidth capability of MRs Internet.

Above flow chart explains the selection of efficient mobile router using TD in order to provide internet services to all mobile routers in optimize manner as well as prevent from looping (**Figure 1**).

2.3. Advertises Availability of MRs

Second level of NEMO+ protocol is Network in Node Advertisement (NINA) which is used to ensure the routes of all MN through EFNEMO are enclosed in a tree structure. MR runs the NINA protocol that rely upon RA+TIO, which in turn MR responds to source of RA+TIO with NINA response, which contains all the details of previous information that currently maintained by MR. Once receiving the NINA response, source of RA+TIO starts forwarding the NINA message to current attachment of MR; It contains both the prefix of MR which is already maintained and the prefix of MR that are currently attached. The process is repeated until top of the tree is reached in EFNEMO+ *i.e*. Process is repeated until entire MR is appraised that are connected in EFNEMO+. As with TD, NINA inherits behavior of EFNEMO MRs by augmenting the NA with NINO (Network in Node Option) messages. TD augments RA messages to act MR as mobile router to its ingress interface. When MR ingress interfaces, it acts itself as individual host, advertisement is done by itself using NA message and it carries information about network prefix to reach itself in these NA message by single node advertisement. An effective technique Route propagation model is engaged in NINA for frequent updates of MR. NINA will hide the changes in the topological structure of MR and to endure the reachability of MR it will also hide the

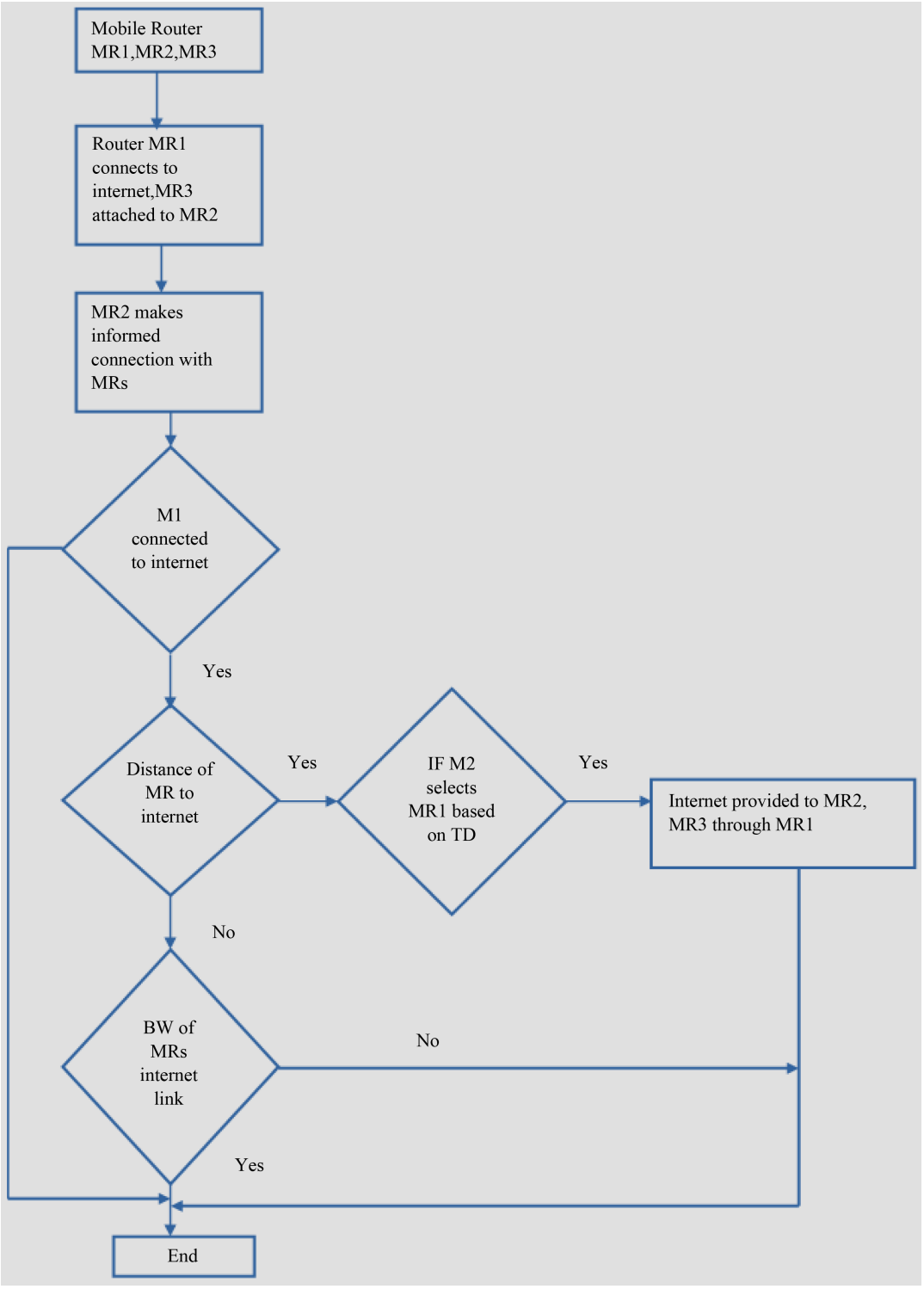

Figure 1. Flow chart representation of MR selection using TD.

movements of sub tree from parent sub tree in Ingress interface of MR. As a result, the MR which is closer to gateway-MR is observed less for MR mobility, the routes are maintained for more prefixes. Meanwhile the MR which is far away from gateway-MR will observe more for mobility of MR and the routes are maintained for less prefixes.

2.4. Ensuring the Packet Delivery

To ensure the efficient delivery of the packets beyond the Gateway-MR, a Reverse Routing header (RRH) protocol is introduced to prevent occurrence of pinball routing. In RRH each MR in the EFNEMO update their HA with current location of the gateway-MR, to ensure the direct delivery of packets to their current location, this is achieved by combining the source routing protocol in EFNEMO with traditional IP routing. As the packets travels towards internet, RRH record the routes of the packets flow. This is done when each MR overwrites the source filed of the outer IPV6 header of the travelled packets and overwrites the existing source addresses are recorded. By this, each MR sends the packets to its actual COA of the gateway-MR as it is source address and the routes are taken back to reach the actual MR by RRH method. This information is stored in HA and successively assigns the destination of the outer IPV6 header to the Gateway-MR COA and RRH is set to the packets to transmit from CN to MR. Before the packets are delivered to destination COA that are recorded in RRH, it first delivers to its Gateway-MR COA.

If NINA is not present, RRH is designed to record the path through the EFNEMO. When NINA is supported by MR, then role of RRH has to record the actual COA of the MR and check correctness of topology in Gateway-MR COA and report it to MRs HA. In the return flow of communication HA to MR, MR acts as a destination COA and the packet will be routed using the NINA protocol.

2.5. Handover in EFNEMO+

During handover, the MR discover the entire MR's in the ingress interface network and sends the NINA message to each egress interface of MR that advertised about the subsequent flow of routes in the MR. The handover operation is divided in two modes predictive (**Figure 2**) and reactive mode (**Figure 3**) based on Fback (Fback) message that are received in previous link. Whenever trigger happens in layer2 it initiates the predictive handover. When MR receive acknowledgement (PrRtAdv) from HA, MR then creates NCoA for registration. In EFNEMO+ for enumerated handover operation and successions timing; it will not send Tentative Binding Update (TBU) message, instead of that, TBU message is entrenched in the FBU message; to register NCoA is in advance. These TBU message is encrypted using ECC conveyed to HA through FBU and HI message.

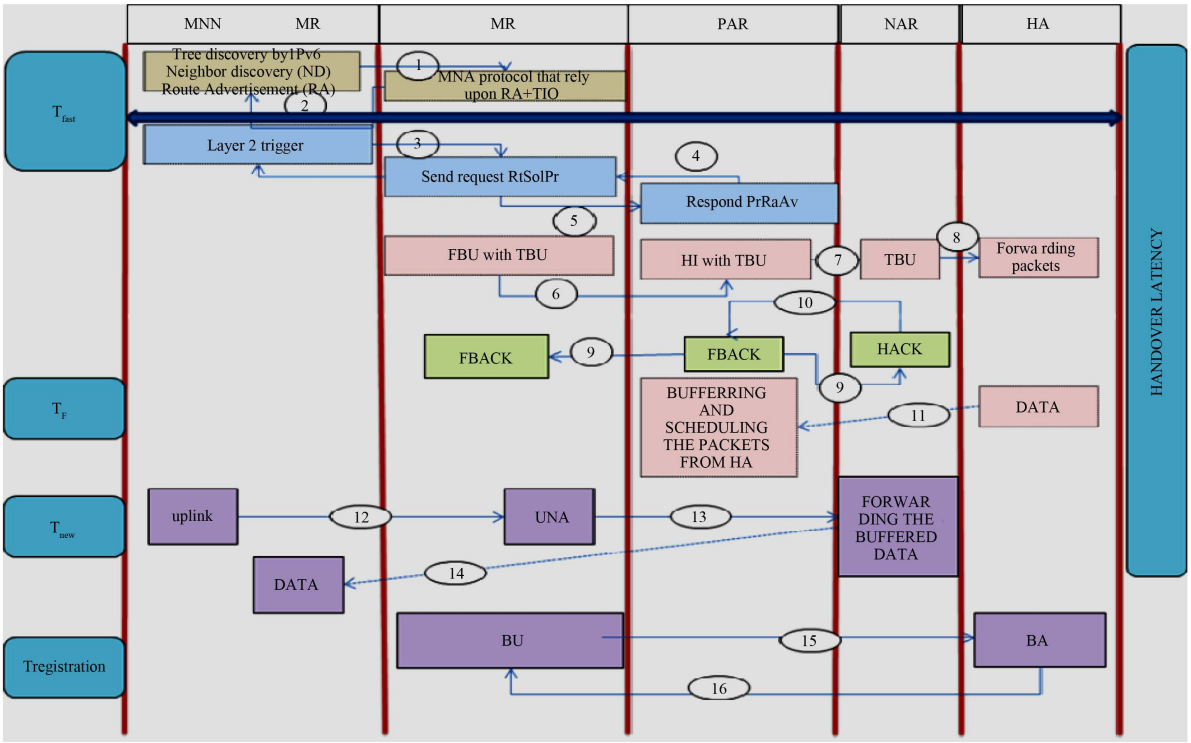

Figure 2. Handover mechanisms in predictive mode.

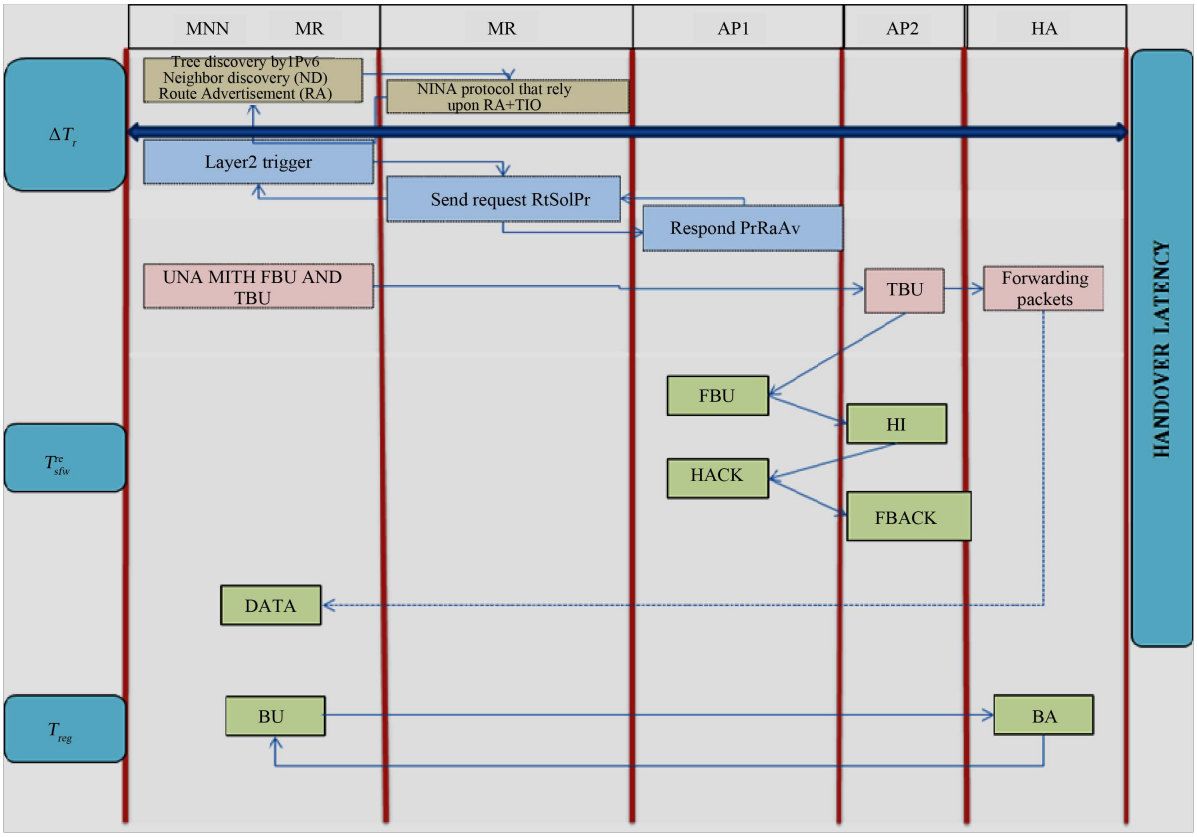

Figure 3. Handover mechanisms in reactive mode.

After receiving the acknowledgement from CN, HA probably use binding information to create an extra entry in the Binding Cache Entry (BCE) for coexisting MR's HoA. To stay away from the Ping-Pong impact, during handover HA forward the packets to PAR because MR does not move to the NAR after sending TBU message to HA. TBU message contains address of MR's HoA, the NCoA, and the short binding lifetime.

In order to avoid burrow burden between PAR and NAR, NAR starts buffering the packets which are sent from HA, and from NAR it reaches destined MNN through various paths. In EFNEMO+, the burrow between the PAR and the NAR still remains, the burrow is used when the HA can't handle the TBU message, or the TBU message is not conveyed to NAR. After handover process in Layer-2, through normal BU message MR registers the NCoA with HA and updates it in BCE. Before handlayer2 happens MR has to receive the Fback message from HA to continue in predictive mode else EFNEMO+ operates in reactive mode. In reactive mode activates, after layer2 handover is completed; then MR sends the UNA (Unsolicited Neighbor Advertisement) is embedded in FBU to NAR. Then PAR receives the FBU message from NAR. HI, HACK messages are exchanged between PAR and NAR, which creates burrow to forward the packets when Hack message is received by PAR and sends the Fback message to NAR. The packets are delivered to MNN before registering NCoA. Burrow is used to deliver the packets between MNN and HA, When TBU message is not accomplished in predictive mode

2.6. Handover in Multihomed Network

Multi homing refers to the phenomena of one network end node accesses to the Internet uses multiple network paths to accesses the Internet, it consider the fault resilience. The multi homed network end node habitually possesses several addresses to access the internet via multiple path networks *i.e*. if the current network path fails, it can immediately switch to another address and another network path for communication. EFNEMO+ efficient handover mechanism is introduced in multi homed mobility configuration based on flow binding to access the destination network from multiple networks (**Figure 4**). It predicts the handover by using the actual location information and previously recorded context data. It has three main functions for predictive handover:

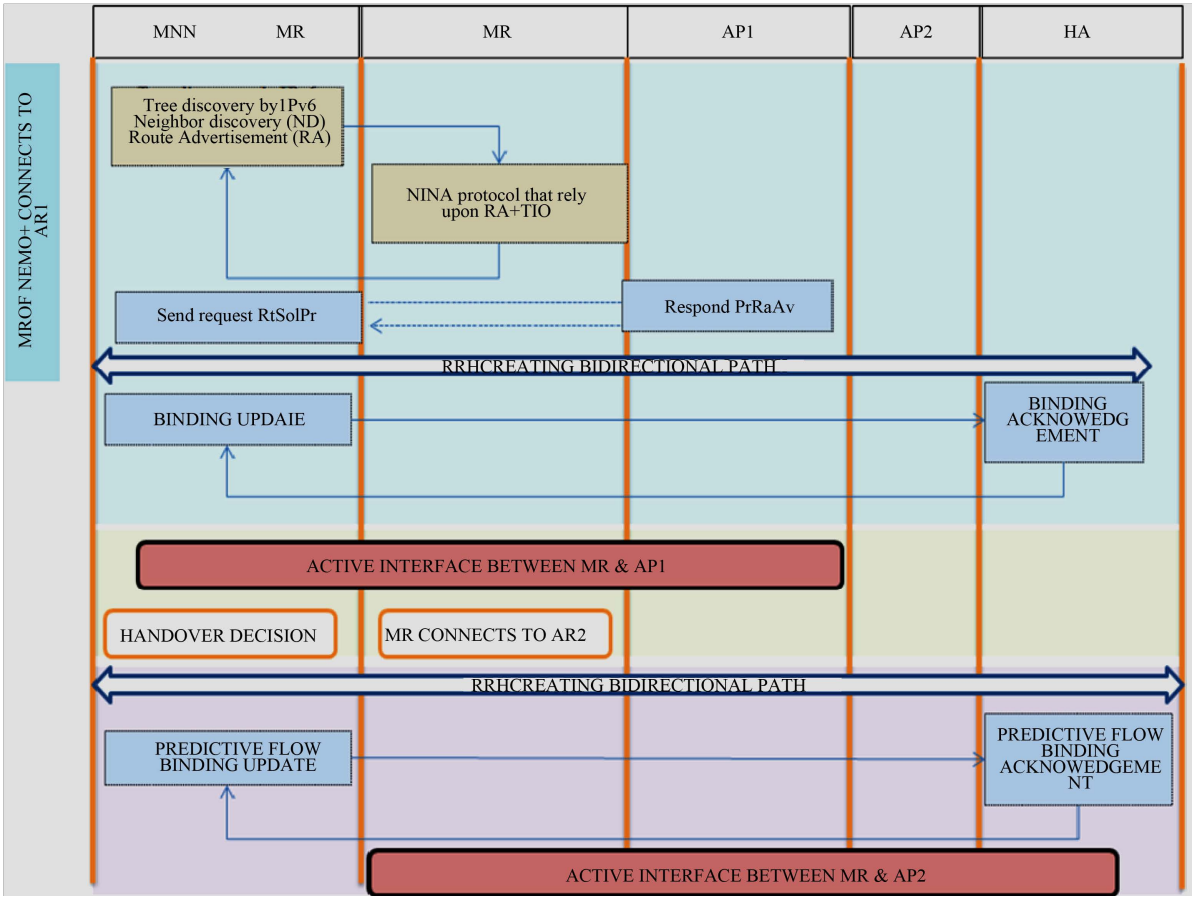

Figure 4. Handover mechanisms in heterogeneous network.

- Access Network Prediction (ANP)
- MR's Handover Manager (HM-MR)
- Home Agent (HM-HA)

2.7. Security during Handover

To ensure the secure transmission of BU data from the adversary attack the Elliptic Curve Cryptographic system (ECC) [28] and the Elliptic Curve Digital Signature Algorithm (ECDSA) [29] are adopted to provide protection for the BU messages.

In this paper, CN stay away from false binding; the reachability of MR and address proprietorship of MN is verified. Address of the MR is created by 128-bit NEMO+ based on MR's private key and one way hash function is compute for authenticating the authority of MR's. By using MR's private key and a valid subnet prefix, the proprietorship of MR's IP address is verified by CN.

Second reachability of MR is verified in PKBU. In this method, MA sends the hash value of the MR's HoA, the public key of MR, and request for the CN's public key to the CN through HA. Once MR receives the CN's Public key, the messages are sent directly to CN; by using CN's Public key MR encrypts the MR's COA and HOA in the message. When message are delivered to CN, it uses the MR's public key to verify the signature, and then MN's CoA and HoA is gained after decrypting the message. Then CN compares the hash value of HoA with hash value of the received message from MR. While checking and the validating the MR's HoA and CoA is result in positive, then the CN allows MR to register in that CoA.

Exchange of messages between the nodes in the PKBU protocol involves three stages. In Stage 1 the proprietorship of the MR's IP address which involves three strides. In Stage 2, the reachability of MR is verified. Stage 3 is validation process which consists of four strides. During validation process CN has to ensure the proprie-

torship of MR and reachability of HoA and CoA.

Stage 1: Proprietorship of the MR's IP

In this stage, MR generates its private, public key and interface ID in 3 strides (**Figure 5**).

1) Creating private key:

MR's private key is generated by user identity number (UI) is an integer. A hash function with randomly generated integer of an UI is calculated to produce MR's private key as follows,

$$\mathrm{MR}_{\mathrm{PR}} = \mathrm{Hash}(\mathrm{UI}) * \mathrm{m}$$

where, $\mathrm{MN}_{\mathrm{PR}}$ is MR Private Key and m is a random integer ranges from1 to n-1.Since it is secure the ambiguities value cannot predicted.

2) Creating public key:

In this process, MR creates its own public key. Using ECC the public key of MR is generated with the MR's private key. Consider the equation C: $y2 = x3 + ax + b$, where (x, y) are points on the curve, and b values generated for curve. The bounds of ECC are B= {a, b, P, m} where a, b are values of the elliptic curve, P is base point of elliptic curve and m is the order of curves. MR's public key $(\mathrm{MR}_{\mathrm{PU}})$ is generated using the MR's private key $(\mathrm{MR}_{\mathrm{PR}})$ and then MR's public key $(\mathrm{MR}_{\mathrm{PU}})$ is $(\mathrm{MR}_{\mathrm{PR}} \cdot \mathrm{P})$ is a point on C. Therefore $\mathrm{MR}_{\mathrm{PU}}$ is point on the curve that is generated by private key. To check the proprietorship of the MR's IP address has both Public key and Private Key.

$$\mathrm{MR}_{\mathrm{PU}} = \mathrm{MR}_{\mathrm{PR}} \cdot \mathrm{P}$$

3) Creating Interface ID:

In this step, Interface ID is created as 128 bit address, 64 bit given for subnet prefix and 64-bit for interface identifier that are derived from hash value of MR's private key. This method creates secure binding between MR's Interface ID and its own Private Key without involving PKI.

Stage 2: Reachability of the MR to CN

Reachability of MR is achieved by sending the CoA to CN through HA by way of IP sec. whenever MR enter into new network it must register with new CoA and the operation on HA is completed before MR uses new CoA. The following steps are to ensure the reachability of MR to CN.

Step 1: MR sends message to CN: MR sends the requirements for routing optimization to CN through HA. In the pre-established burrow MR sends Hash values of MR's HoA, public key of MR, and requests the public key of CN through HA to CN.

Step 2: CN sends messages to MR: CN responds accordance with request of MR. That is MR receives the CN public key by HA; Hash values of MR's HoA and MR's public are stored in CN.

Step 3: Encryption of message in MR: Using CN's public key the MR encrypts the MR's CoA and HoA and these cipher text are signed using MR's private key.

Stage 3: Validation Process

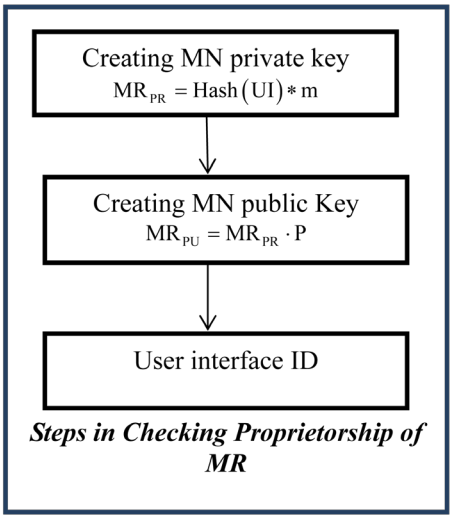

Figure 5. Checking MN proprietorship.

In this stage it validate the process the requirements for security, proprietorship, and reachability of the MN's IP addresses. CN authenticate the MR signature by using the MR's private key. If the sign is not done using the MR's private key then the process is tends to end. After authenticating the signature, CN checks the message confidentiality by decrypting with the CN private key to gain MR's CoA and HoA. CN assures the HoA by calculating the hash value of decrypted HoA and the results is compared with the hash value of HoA which are sent by MR. If it results in negative then the message will be prohibited or else if the validate process is result in positive then it approves the proprietorship of MR and when CoA is identified then the MR is reachable to CN will send the binding acknowledgement (BA) message to MR.

The working process of the proposed SEFMNEMO+ algorithm based on the vertical handover mechanism is represented in the form of flow graph (**Figure 6**).

SEFMNEMO+ Algorithm:

Input: Handovers, Hacking the FBU message
Output: Produce seamless connectivity with reduce delay and loss in packet, secures over the transmission of FBU message.
Begin:
For each MR in the network
Discover and connects MRs using tree discovery.
Ensure the routes of connected MR sending the NINA message.
If NINA present then
Trace the path of destined MNN
Else
Record the actual CoA of MR .
End If
End for
// HANDOVER PROCESS****
For each time handover
If FBack received before trigger of layer 2 then
MR→RtSolPr to PAR
Until (MR←PrRtAdv)
// Proprietorship of the MR's IP****
$MR_{PR} = \text{Hash}(UI) * m$
$MR_{PU} = MR_{PR} \cdot P$
UID←128 bit address
//Reachability of the MR to CN****
For MR to CN then
MR(CoA) →Hash (MR (HoA)), MNPUK, ReqCNPUK→**HA**
HA→Hash (MN (HoA)), MNPUK, ReqCNPUK→**CN**

CNA→CN_{PUK}→**MN**

MN (CoA) →SignMR(PRK) (EncryptCN(PUK) (MN(CoA), MN (HoA))) →**CN**
If (MNN receive BU) then
Advance registration ←NCoA.
End If
BCE[]←MR's HoA

BUFFERING THE PACKETS TO NAR**
For N=0 to n-1
NARbuf[]←packets from HA
End if
SEND THE BUFFERED PACKETS TO MNN**
For ∀ packets in NARbuf[]
NARbuf[]→packets to MNN.
End for
Else
// Proprietorship of the MR's IP****
$MR_{PR} = \text{Hash}(UI) * m$
$MR_{PU} = MR_{PR} \cdot P$
User interface ID←128 bit address
//Reachability of the MR to CN****
For MR to CN
MR(CoA)→Hash (MR (HoA)), MNPUK, ReqCNPUK→**HA**
HA→Hash (MN (HoA)), MNPUK, ReqCNPUK→**CN**
CN→CN_{PUK}→HA
HA→CN_{PUK}→MN
MN (CoA)→SignMR(PRK)
(EncryptCN(PUK)(MN(CoA), MN (HoA)))→CN
If (MNN receive BU) then
Sends UNA message to PAR
Until (NAR receives ACK)
** exchanging HI and HACK message **
NAR→HI to PAR
PAR→HACK to NAR

End

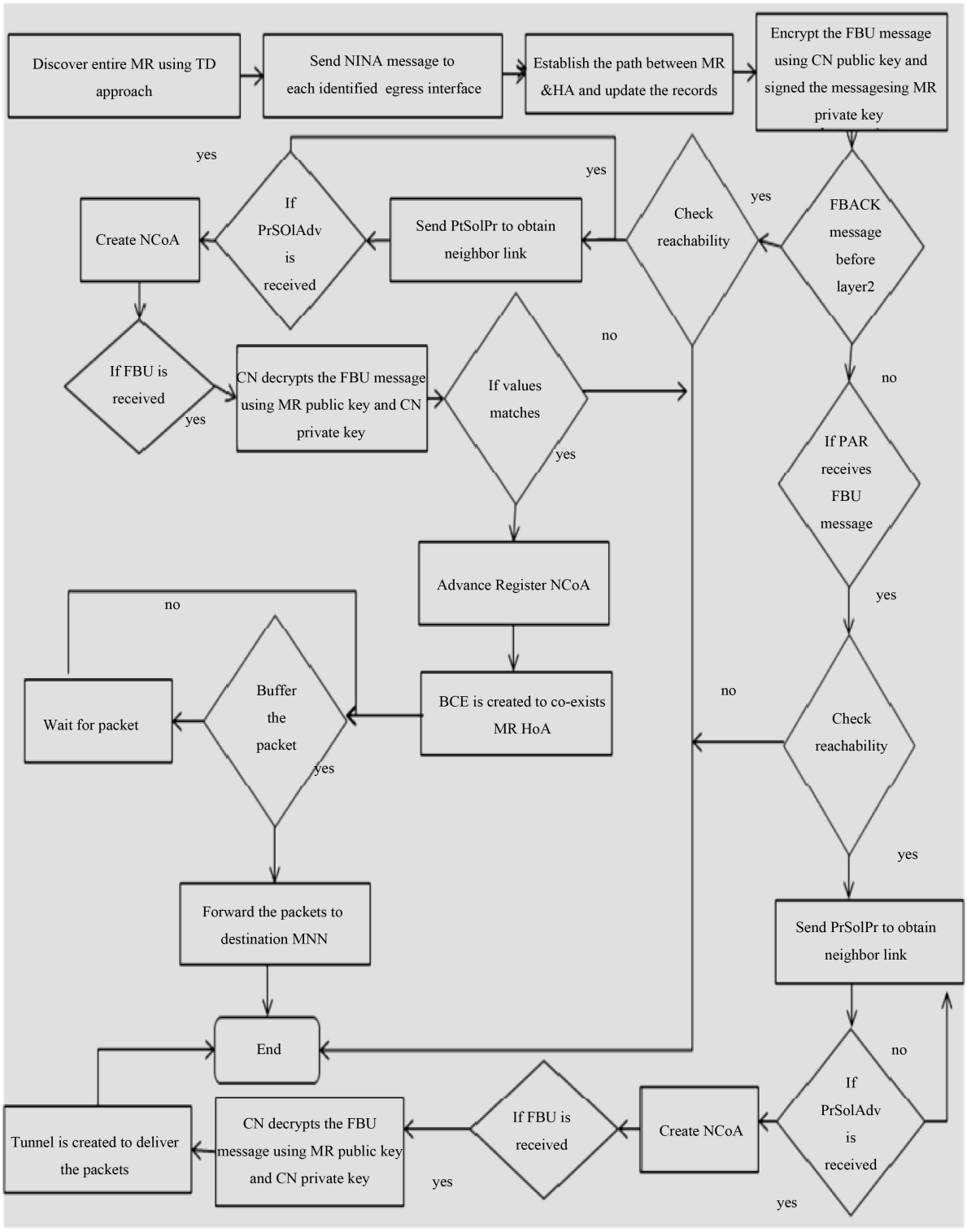

Figure 6. Flow graph of SEFMNEMO+.

3. Experimental Analysis

In the experimental analysis, it analyzes the security, handover efficiency and its performance is analyzed using proposed methodology. The proposed methodology is implemented using NS-2 network simulator tool with a

network capacity of 100 mobiles nodes. The simulation is tested for the performance of the handover rate in NEMO+, EFNEMO+, SEFMNEMO+ with the given network capacity.

The simulation parameters are used while implementing this proposed technique, which is summarized below in **Table 1**. These parameters are used for constructing the network.

3.1. Evaluation Metrics

The performance of this work is measured using packet loss, average delay, control overhead and average throughput which shows that an efficient result of proposed protocol when compared with existing system. These results are discussed briefly below.

3.1.1. Packet Loss Ratio (PLR)

PLR is defined as rate of Number of message received in a packet at the destination by Total number of message sent from source while handover process is taken place. The PLR is measured using following formula.

$$\text{PLR} = \frac{\text{sum}\left(\text{Number of packet receive after handover}\right)}{\text{sum}\left(\text{Number of packet send before handover}\right)} \times 100 \quad (1)$$

Figure 7 shows that proposed SEFMNEMO+ has low packet loss than existing approach NEMO+ and EFNEMO+ when handover mechanism occurs between nodes. **Figure 8** shows that proposed SEFMNEMO+ has low packet loss than existing approach NEMO+ and EFNEMO+ under different node velocity. The packet loss ratio is represented by percentage (%).

3.1.2. Average Delay

The average delay is calculated by taking the average of delays for every data packet transmitted to the total number of received packets as defined below in equation. The parameter is measured only when the data transmission has been successful.

Table 1. Simulation parameters.

Simulation Parameter	Value
Propagation	Two Ray Ground
Channel	Wireless Channel
Physical Layer	Wireless Physical
Queue	DropTail/PriQueue
Mac	802_.11
X dimension of the topography	500
Y dimension of the topography	500
Ad hoc Routing	AODV
Antenna	Omni Antenna
Max packet	100
Number of nodes simulated	50
Cp	./cbr
Sc	nodes50
Simulation time	100 s
Energy	Energy Model
Initial Energy	100
Min Neighbor	6
Security Duration	4
Adversary node	5

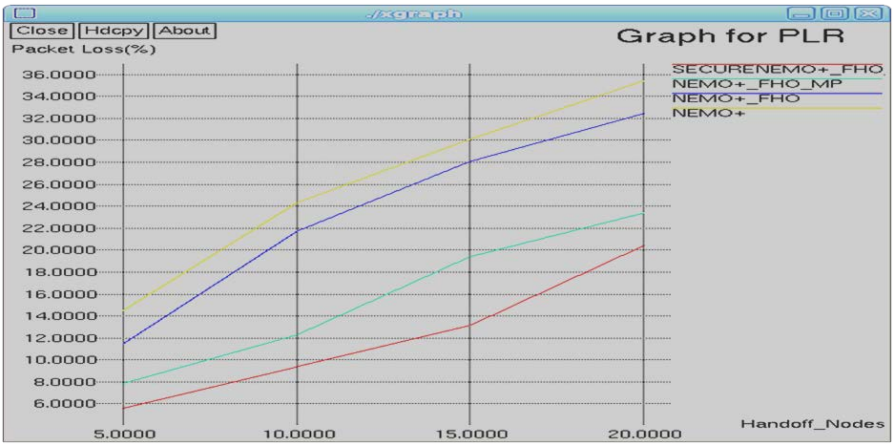

Figure 7. PLR in node (handover).

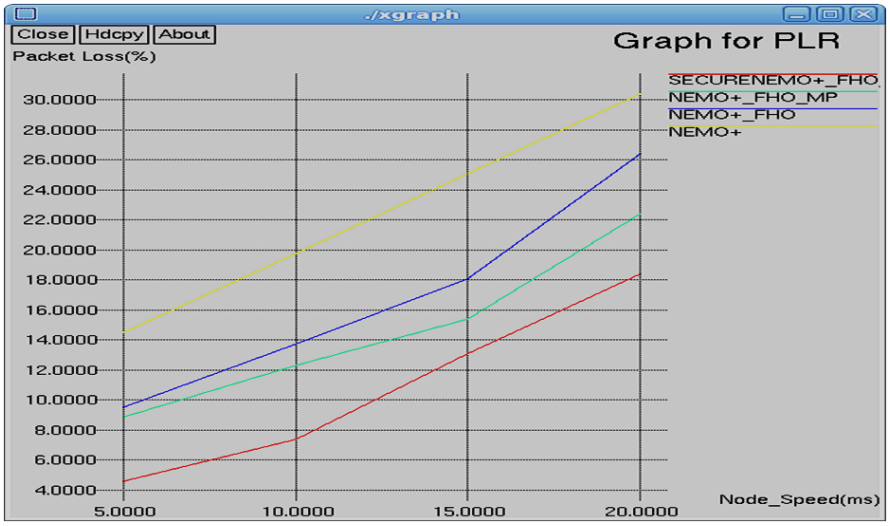

Figure 8. PLR in node (speed).

$$\text{Average Delay} = \frac{\text{Sum of all packets delay}}{\text{Total Number of Received Packets}} \quad (2)$$

Figure 9 shows that proposed SEFMNEMO+ has low average delay than existing approach NEMO+ and EFNEMO+ when handover mechanism occurs between nodes. **Figure 10** shows that proposed SEFMNEMO+ has low average delay than existing approach NEMO+ and EFNEMO+ under different node velocity. The average delay is represented by percentage (ms).

3.1.3. Overhead

The ratio of total numbers of control packets generated to the total number of data packets received during the simulation time given in equation.

$$\text{Overhead} = \frac{\text{data packets received}}{\text{control packets generated}} \quad (3)$$

Figure 11 shows that proposed SEFMNEMO+ has low overhead than existing approach NEMO+ and EFNEMO+ when handover mechanism occurs between nodes. **Figure 12** shows that proposed SEFMNEMO+ has low overhead than existing approach NEMO+ and EFNEMO+ under different node velocity. The overhead is represented by percentage (%).

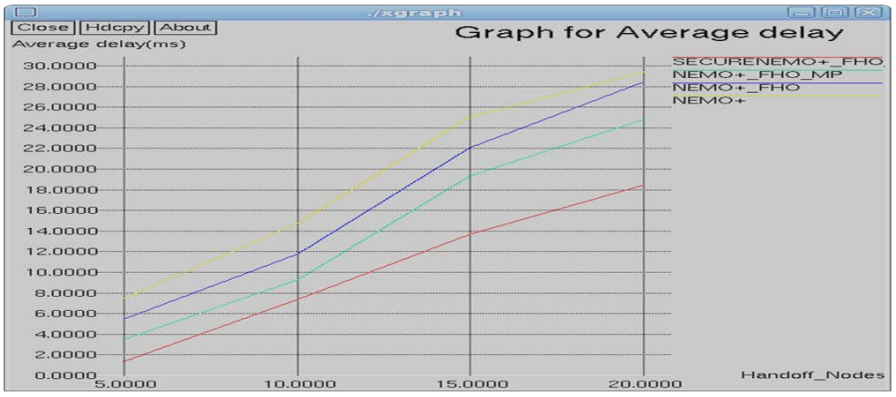

Figure 9. Average delay in node (handover).

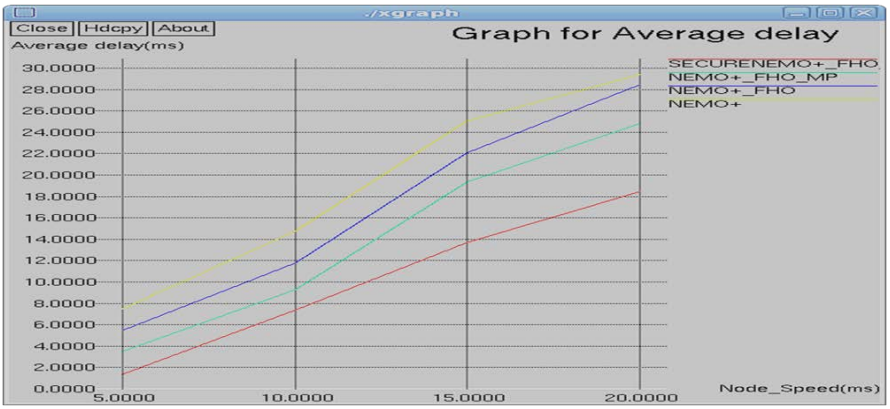

Figure 10. Average delay in node (speed).

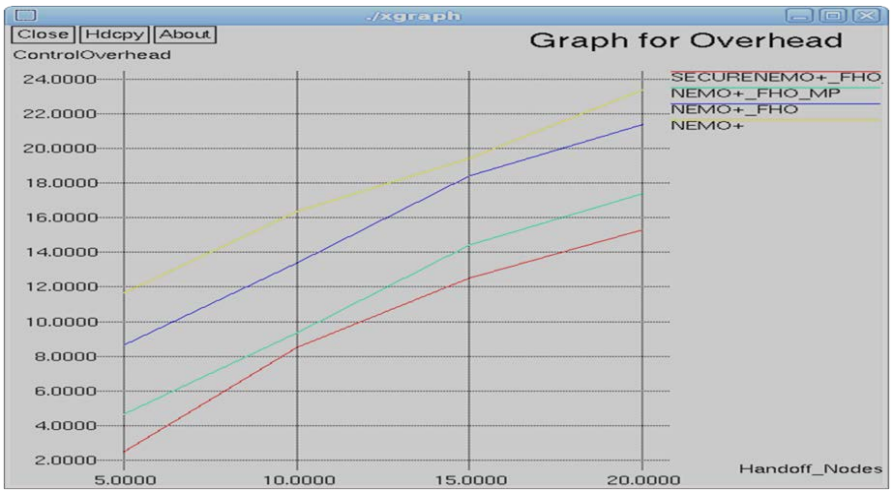

Figure 11. Overhead in node (handover).

3.1.4. Throughput

Throughput is defined as total number of kilobytes by total bytes received per second. It is represented by kbps.

$$\text{Throughput} = \frac{\text{Total number of kilo bytes}}{\text{Total bytes received per second}} \quad (4)$$

Figure 13 shows that proposed SEFMNEMO+ has high throughput than existing approach NEMO+ and

EFNEMO+ when handover mechanism occurs between nodes. **Figure 14** shows that proposed SEFMNEMO+ has high throughput than existing approach NEMO+ and EFNEMO+ under different node velocity.

Figure 14 clearly shows the percentage of improvement achieved for various performance metrics of the proposed technique approach with existing approach. The proposed work improves its performance in all the metrics, where the packet loss is improved much better than NEMO+ and EFNEMO+.

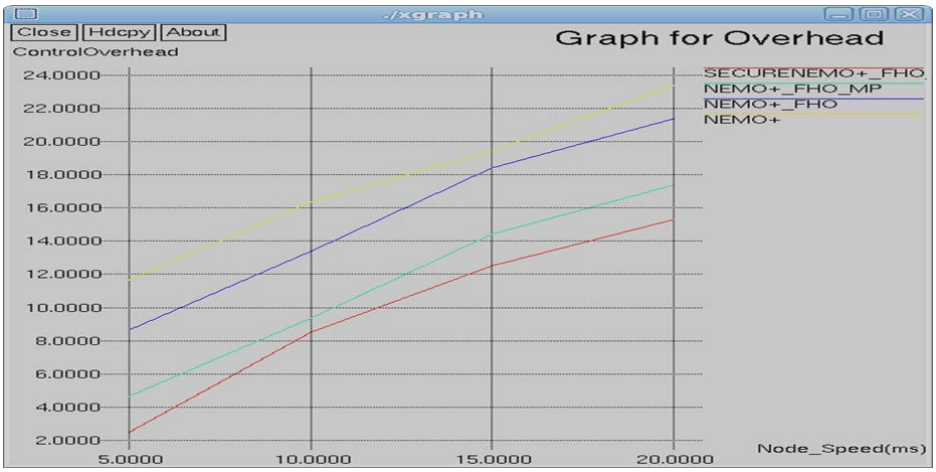

Figure 12. Overhead in node (speed).

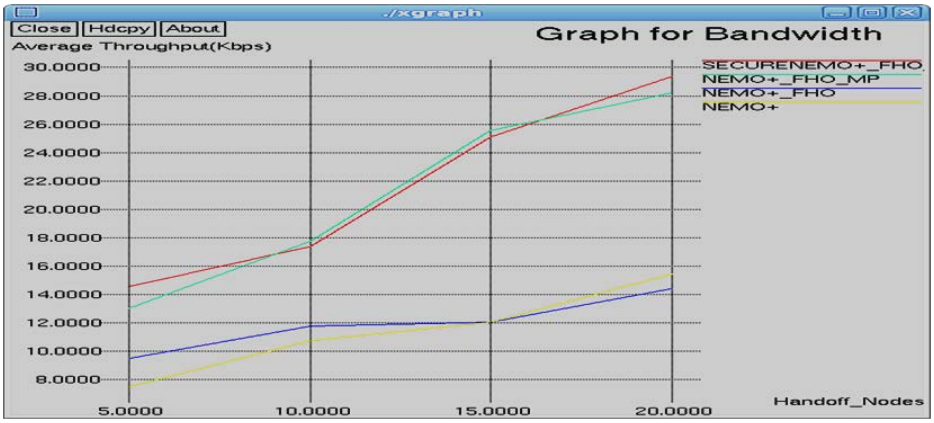

Figure 13. Throughput in node (handover).

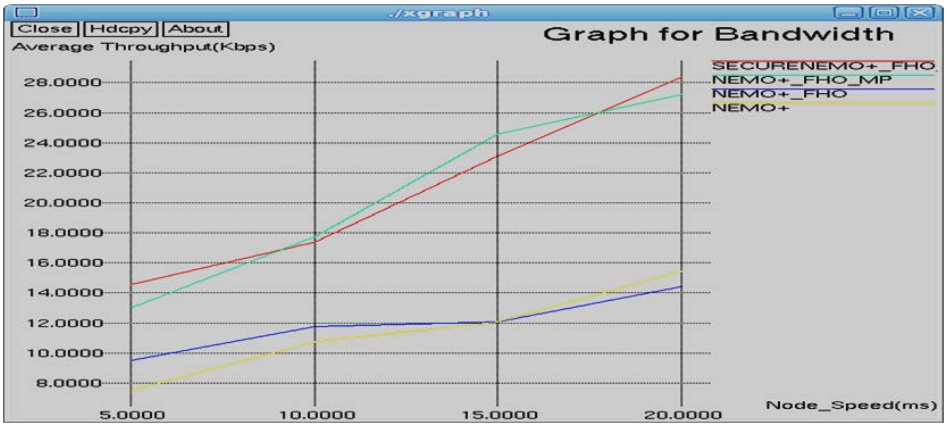

Figure 14. Throughput in node (speed).

4. Conclusion

In VANET, the seamless connectivity is produced during the handover. The proposed framework is used to improve the seamless connectivity by reducing delay and loss of packet and security mechanism among the VANET. It is achieved by hybrid implementation of NEMO+ scheme and public key cryptography for secured efficient handover mechanism. The experimental analysis of proposed framework EFMNEMO+ is being compared with existing NEMO+ and the results show that the average delay, overhead, packet loss are minimum with higher PDR value and higher throughput. SEFMNEMO+ is found to be better in minimizing the average delay and overhead thus reducing the rate of packet loss when compared to NEMO+ or EFNEMO+.

References

[1] Spadafora, W.G., Paielli, P.M., Llewellyn, D.R. and Kramer, J.G. (2010) Intelligent Transportation System. Bosch Rexroth Corporation, United States Patent US 7,689,230.

[2] Vahidi, A. and Eskandarian, A. (2003) Research Advances in Intelligent Collision Avoidance and Adaptive Cruise Control. *IEEE Transactions on Intelligent Transportation Systems*, **4**, 143-153.

[3] Varshney, U. (2003) The Status and Future of 802.11-Based WLANs. *IEEE Transactions on Computer*, **36**, 102-105.

[4] Sun, X. and Li, X.M. (2008) Study of the Feasibility of VANET and Its Routing Protocols. 4*th International Conference on Wireless Communications, Networking and Mobile Computing*, Dalian, 12-14 October 2008, 1-4.

[5] Liu, Y., Bi, J. and Yang, J. (2009) Research on Vehicular Ad Hoc Networks. *Chinese Control and Decision Conference*, Guilin, 17-19 June 2009, 4430-4435.

[6] Céspedes, S., Shen, X. and Lazo, C. (2011) IP Mobility Management for Vehicular Communication Networks: Challenges and Solutions. *IEEE Communications Magazine*, **49**, 187-194. http://dx.doi.org/10.1109/MCOM.2011.5762817

[7] Paul, B., *et al*. (2012) Vanet Routing Protocols: Pros and Cons. arXiv preprint arXiv: 1204.1201.

[8] Nzouonta, J., *et al*. (2009) VANET Routing on City Roads Using Real-Time Vehicular Traffic Information. *IEEE Transactions on Vehicular Technology*, **58**, 3609-3626.

[9] Francis, P., *et al.* (1999) An Architecture for a Global Internet Host Distance Estimation Service. *Proceedings of* 18*th Annual Joint Conference of the IEEE Computer and Communications Societies*, New York, 21-25 March 1999, Vol. 1: 210-217. http://dx.doi.org/10.1109/infcom.1999.749285

[10] Tseng, Y.-C., Ni, S.Y. and Shih, E.-Y. (2003) Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad Hoc Network. *IEEE Transactions on Computers*, **52**, 545-557. http://dx.doi.org/10.1109/TC.2003.1197122

[11] Lin, Y.-D. and Hsu, Y.-C. (2000) Multihop Cellular: A New Architecture for Wireless Communications. *Proceedings of* 19*th Annual Joint Conference of the IEEE Computer and Communications Societies*, Tel Aviv, 26-30 March 2000, 1273-1282.

[12] Baldessari, R., Festag, A. and Abeillé, J. (2007) NEMO Meets VANET: A Deployability Analysis of Network Mobility in Vehicular Communication. 7*th International Conference on ITS Telecommunications*, Sophia Antipolis, 6-8 June 2007, 1-6. http://dx.doi.org/10.1109/itst.2007.4295897

[13] Leung, K., Dommety, G., Narayanan, V. and Petrescu, A. (2008) Network Mobility (NEMO) Extensions for Mobile IPv4. April 2008, RFC6626,RFC 5177 Proposed Standard.

[14] Bernardos, C.J., Gramaglia, M., Contreras, L.M., Calderon, M. and Soto, I. (2010) Network-Based Localized IP Mobility Management: Proxy Mobile IPv6 and Current Trends in Standardization. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Application*, **1**, 16-35.

[15] Soto, I., Bernardos, C.J., Calderon, M., Banchs, A. and Azcorra, A. (2009) NEMO-Enabled Localized Mobility Support for Internet Access in Automotive Scenarios. *IEEE Communications Magazine*, **47**, 152-159. http://dx.doi.org/10.1109/MCOM.2009.4939291

[16] Bascom, W. (1961) The Ocean Is Huge, Powerful, and Eternal. Puny Man Can Scarcely Expect to Win by Overwhelming It, and Anyone Who Counters Its Attack with Brute-Force Solutions Is Doomed to Expensive Disappointment. Minot Beach Community Scituate, MA 2010.

[17] Basak, R. and Sardar, B. (2013) Security in Network Mobility (NEMO): Issues, Solutions, Classification, Evaluation, and Future Research Directions. *Network Protocols and Algorithms*, **5**, 87-111. http://dx.doi.org/10.5296/npa.v5i3.3789

[18] McCarthy, B., Jakeman, M., Edwards, C. and Thubert, P. (2008) Protocols to Efficiently Support Nested NEMO (NEMO+). *Proceedings of the* 3*rd International Workshop on Mobility in the Evolving Internet Architecture*, Seattle, 22 August 2008, 43-48. http://dx.doi.org/10.1145/1403007.1403018

[19] Ryu, S., Park, K.J. and Choi, J.W. (2014) Enhanced Fast Handover for Network Mobility in Intelligent Transportation Systems. *IEEE Transactions on Vehicular Technology*, **63**, 357-371. http://dx.doi.org/10.1109/TVT.2013.2272059

[20] Ryu, S., Choi, J.-W. and Park, K.-J. (2012) A Scheme Improving Fast PMIPv6-Based Network Mobility by Eliminating Tunneling Overload for ITS. *Proceedings of the* 2012 *IEEE Intelligent Vehicles Symposium Workshops*, June 2012, 1-6.

[21] Zao, J., Gahm, J., Troxel, G., Condell, M., Helinek, P., Yuan, N., Castineyra, I. and Kent, S. (1999) A Public-Key Based Secure Mobile IP. *Wireless Networks*, **5**, 373-390. http://dx.doi.org/10.1023/A:1019179817993

[22] Benantar, M. (2001) Method and System for Public-Key-Based Secure Authentication to Distributed Legacy Applications. United States Patent Application US 09/821,079.

[23] Taleb, T., Sakhaee, E., Jamalipour, A., Hashimoto, K., Kato, N. and Nemoto, Y. (2007) A Stable Routing Protocol to Support ITS Services in VANET Networks. *IEEE Transactions on Vehicular Technology*, **56**, 3337-3347. http://dx.doi.org/10.1109/TVT.2007.906873

[24] TamilSelvan, M.D., Vasudevan, V., Parasuraman, P.R. and Aadhimoolam, A.V. (2014) Mobility Prediction and Node Prediction Based Light-Weight Reliable Broadcast Message Delivery for Vehicular Ad-Hoc Networks. *International Journal of Advanced Research in Computer and Communication Engineering*, **3**, 5321-5325.

[25] Lee, D., Kim, Y.H. and Lee, H. (2014) Route Prediction Based Vehicular Mobility Management Scheme for VANET. *International Journal of Distributed Sensor Networks*, **2014**, Article ID: 679780. http://dx.doi.org/10.1155/2014/679780

[26] Park, H.D., Kum, D.W., Kwon, Y.H., Lee, K.W. and Cho, Y.Z. (2006) IP Mobility Support with a Multihomed Mobile Router. In: Boavida, F., Plagemann, T., Stiller, B., Westphal, C. and Monteiro, E., Eds., *NETWORKING* 2006. *Networking Technologies, Services, and Protocols*; *Performance of Computer and Communication Networks*; *Mobile and Wireless Communications Systems*, Springer, Berlin Heidelberg, 1144-1149. http://dx.doi.org/10.1007/11753810_100

[27] Im, I., Cho, Y.H., Choi, J.Y. and Jeong, J. (2012) Security-Effective Fast Authentication Mechanism for Network Mobility in Proxy Mobile IPv6 Networks. In: Murgante, B., Gervasi, O., Misra, S., Nedjah, N., Rocha, A.M.A.C., Taniar, D. and Apduhan, B.O., Eds., *Computational Science and Its Applications—ICCSA* 2012, Springer, Berlin Heidelberg, 543-559. http://dx.doi.org/10.1007/978-3-642-31128-4_40

[28] Gura, N., Shantz, S.C., Eberle, H., Gupta, S., Gupta, V., Finchelstein, D., Goupy, E. and Stebila, D. (2003) An End-to-End Systems Approach to Elliptic Curve Cryptography. In: Kaliski, B.S., Koç, Ç.K. and Paar, C., Eds., *Cryptographic Hardware and Embedded Systems—CHES* 2002, Springer, Berlin Heidelberg, 349-365. http://dx.doi.org/10.1007/3-540-36400-5_26

[29] Johnson, D., Menezes, A. and Vanstone, S. (2001) The Elliptic Curve Digital Signature Algorithm (ECDSA). *International Journal of Information Security*, **1**, 36-63. http://dx.doi.org/10.1007/s102070100002