SSI Routing Scheme for Heterogeneous MANETs

Rekha B[1], D.V. Ashoka[2]

[1]Research Scholar, Department of CSE, Jain University Bangalore, India
[2]Prof., Department of ISE, JSSATE, Bangalore, India

***Abstract*— *Studies towards heterogeneous Mobile Adhoc Network (MANET) as well as inter-domain routing is still in much infancy stage. After reviewing the existing literaturs, it was found that problems associated with scalability, interoperability, and security is not defined up to the mark as it should be part of pervasive computing in future networks. Moreover, it was found that existing studies do not consider the complexities associated with heterogeneous MANET to a large extent leading to narrowed research scope. Hence, this paper introduces a novel scheme called as Secure, Scalable and Interoperable (SSI)routing, where a joint algorithm is designed, developed, and implemented. The outcome exhibits the correctness of this scheme by simulation assisted by analysis for inter-domain routing.*

Keywords*— *Heterogeneous Mobile Adhoc Network, Gateway Protocol, Inter-domain Routing, Scalability, Security

I. INTRODUCTION

Mobile Adhoc Network (MANET) has been heard for more than a decade in the research community, where various researchers present their contribution for solving different types of issues such as routing, energy, security load balancing [1][2]. However, problems in MANET are still not solved inspite of massive archival of research manuscripts. A closer look into all the research papers irrespective of the problem will show that majority of the research issues have raised from dynamic topology, intermittent routing, energy dissipation[3]. Majority of the existing study is focused on homogeneous routing techniques whereas the future demands more pervasiveness [4]. Hence, heterogeneous MANET comes into the picture. This concept is quite a hypothetical and doesn't give a sense of heterogeneity in domain management [5]. Nodes within a domain can exercise different routing protocols. This phenomenon is not seemed to be adopted in existing studies towards heterogeneous MANET. Conventional Border Gateway Protocol (BGP), which is more functional over internet-based connection is not appropriate for MANETs [6]. It is essential to adhere to higher degree of scalability, interoperability, and highly resistive of potential threats. The proposed addresses this problem and provides a balance among scalability, interoperability, and security.

II. RELATED WORK

The work of [6] limits scalability feature and emphasizes on formulation of gateway selection process. The most recent work carried out by Wu et al. [7] has investigated on scalability problem associated with heterogeneous MANETs. The authors have introduced layered-based transmission scheme along with stochastic geometrical approach considering a case study of video coding. Work by Comarela et al. [8] used over software framework like MapReduce mainly looks for the internet-based connections. The reason for intermittent path was addressed in the work carried out by Javed et al. [9] to a large extent. The authors have presented an algorithm that is capable of identifying any sorts of changes over the inter-domain path. Khudayer and Kadhum [10] have presented an analysis to prove that conventional Dynamic Source Routing. Study towards scalability issues was also carried by Pan et al. [11] for internet architecture. Elmokashfi et al. [12] have introduced a toolbox responsible for maintaining scalability in inter-domain routing. Work on inter-domain routing in MANET was carried out by Dressler et al. [13]. The technique has used bio-inspired algorithm for optimizing the inter-domain communication channel. Lee et al. [14] have completely focused on heterogeneous MANETs using property, symbolic name to develop a node parameter in order to permit dynamic merging and splitting of network topologies. Han et al. [15] have presented work focusing on the issue of resource allocation over adhoc network. Durresi et al. [16] have presented an unique architecture meant for hierarchical networking application. The authors have also developed a gateway module for performing translation of different communication protocol. Natarajan and Rajendran [17] have developed a hybrid routing protocol on the basis of shortest path technique. The technique also addresses the energy problems of node and integrates both on-demand and reactive features. Zhu et al. [18] have also presented a study in order to address the scalability problem in inter-domain routing. Souto et al. [19] have developed a framework meant for enhancing the communication system aided by heterogeneous wireless networks. Saluja and Shrivastava [20] have introduced a unique analysis for letting the TCP based connection over mobile adhoc network.

III. PROPOSED SYSTEM

The technique preliminary builds multiple domains with one gateway node within it. Channel state information data is used to identify the best possible condition of routing while channel correlation data is used to enhance the data quality in the network. SSI introduces a novel gateway node that is responsible for performing data conversion process in order to perform inter-domain routing over multiple and different routing protocols. The algorithm of the proposed system supports both on-demand and table-driven approach. The schematic diagram of the SSI scheme is shown in Figure.1.

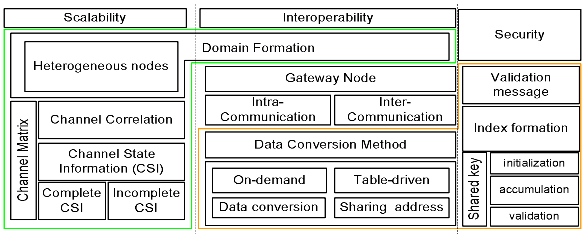

Fig.1: Schematic diagram of SSI

IV. METHODOLOGY

a. Methodology for Ensuring Scalability

The proposed system uses a mechanism by which all the domains along with the mobile nodes within it has to share the information in order to formulate three essential blocks (Figure.2) i.e. channel matrix, correlation matrix, and Channel State Information (CSI) status. Channel matrix basically posses various types of channel-related information (e.g. bandwidth, memory, stability, bottleneck etc.) which are mainly of scalar type of data. Hence, the study uses hessian matrix H to represent it. Correlation matrix is formed by evaluating the similarity measure of the routing message among different domains. This matrix not only reduces redundant information, but also ensured faster processing. CSI information assists in understanding the impact of scattering, fading, interference etc.

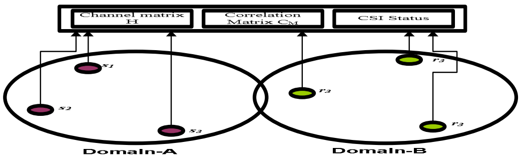

Fig.2 : Scheme of scalability in SSI

Each node in a network broadcast its joining request. One the destination (or an intermediate node) received this message; it decides whether to join the network or to reject it. By this, it maintains its neighbors. The next step is to perform exchanging of the data. In order to do so, each node accesses its own as well as its neighbor channel matrix, correlational matrix, as well as CSI information, which acts as a decision factor to join the network. However, dissemination of channel correlation operation is a computationally complex process for any node in dense network. Hence, this problem is solved using CSI information. Hence, the study uses correlational matrix as well as CSI data in order to get complete information of the destination node. It is to be noted that channel matrix is also responsible to retaining transition state of network topological information, which is maintained inside gateway node. The technique only allows the computation of correlational matrix and CSI state for the communicating nodes and thereby saving energy of the nodes.

b. Methodology for Ensuring Interoperability

This part of the design introduced a gateway node, which will be responsible for i) searching the queried destination node, ii) update synchronous state with other gateway node, iii) carry out data transformation for heterogeneous routing protocol. A gateway node doesn't have any constraint of the resources and hence the proposed study incorporates novelty by shifting some of the operations to be carried out by nodes in conventional system to gateway node. This methodology has certain positive effect e.g. i) lower load of traffic and data processing in mobile nodes, ii) conservation of data, iii) reduction of retransmission due to minimal attempt of search, iv) reliable network due to self-synchronization of all the gateway nodes.

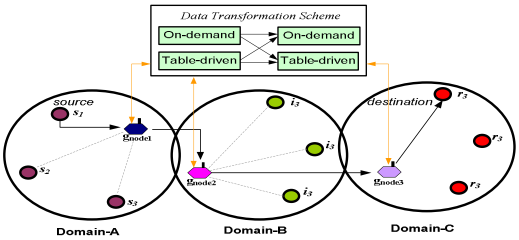

Fig.3: Scheme of interoperability in SSI

The data transformation scheme supports both on-demand and table-driven routing protocol only (Figure.3). As the gateway node has direct access to the address and positional information of the mobile nodes within its range, hence, it can ensure the reachability for any node within or outside of its domain. This characteristics of the communication is used for developing the proposed gateway node to ensure better interoperability among the node communication in heterogeneous MANET.

c. Methodology for Ensuring Security

SSI scheme designs a simple lightweight technique that can validate the legitimacy of the control message being originating from any node or from any domain. The technique uses a novel concept of index and control message which is forwarded to the destination node along with a new validation message. It ensures that in order to decrypt this message, the destination node will require to change the index of the message for which it will also need to spend some resources. Hence, it is quite obvious that probability of malicious node to change the index will be very low compared to legitimate nodes. Hence, if the index is found to be unchanged, the system denies the access considering it as malicious nodes. On the other hand, upon identification of legitimate node, the technique performs sequential encoding operation with simple mathematical operation.

V. ALGORITHM IMPLEMENTATION

There are three different algorithms responsible for implementation of proposed SSI. The first algorithm ensures about scalability, second algorithm for interoperability, and the third algorithm towards ensuring security over heterogeneous mobile adhoc network.

i) Algorithm for Ensuring Scalability

The prime motive of this algorithm is to ensure enough scalability in the process of inter-domain in heterogeneous MANET. The signal vector of receiver is given as

$$r=Hs+n$$

where *r* is a set of receiver and *s* is a set of source node located in two different domains, H is the Hessian matrix developed to represent a channel. It considers Gaussian noise *n* in consideration. Hence, receiver node will be responsible for performing this computation (Line-3). For better analysis, a correlation matrix C_M is designed (A correlation matrix has all the diagonal elements as one with each element above and below the diagonal in the form of CC) (Line-4). The system then checks for the availability of the CSI information, which can be further classifier in two more sub-cased viz. i) scenario with complete availability of CSI (Line-5) and ii) scenario without complete CSI (Line-6). The proposed study also consider a case of optimal channel gain which gives better value of signal attenuation as well as patterns of phase shift angle during dynamic mobility. The study considers selection of a specific node *m** (from *M* (set of nodes)) on the basis of condition stated in Line-5. The entire process is iterated to ensure that all participating nodes are chosen. However, there may be a situation when complete CSI information is not available. In such condition, the transmitting node will only posses information related to correlation only for few specific nodes. Therefore, in this case, we replace *H* with C_M (Line-6). Hence, the algorithm can automatically shift between both the states depending up the situation. The proposed system uses 7 different performance metric e.g. optimal channel gain, channel state information, minimal channel correlation, energy, total delay, bit error rate, and throughput percentage in order to assess its outcome. Apart from it, the study also considers energy efficiency too. The algorithm can compute the entire network lifetime using simplified energy computation between two communication nodes (line-7). The system also performs energy computation considering receiving energy E_r and a new variable φ in order to consider the environmental parameters for a specific distance S_d. Finally, the system considers only the route which has reduced valued of transmittance energy for better path exploration among the different domains in heterogeneous MANET system. The algorithm steps are shown as follows:

Algorithm

```
Input: CC, bt, $S_d$, $S_D$, H, x, r, s, $H_\omega$, $C_M$, $E_{total}$, $E_T$, $E_R$, $\eta$.
Output: path estimation
Start
1. Init $S_d$, $S_D$, bt, s, n
2. Compute Channel Correlation $CC = bt^{\frac{S_d}{S_D}}$
3. $r = Hs + n$
4. $H = H_\omega \,.\, C_M$
5. $m^* = \arg\max_{m^* \in M} \{\det((H^{(x+1)})^H (H^{(x+1)}))\}$
6. $m^* = \arg\max_{m^* \in M} \{\det((C_M{}^{(x+1)})^H (C_M{}^{(x+1)}))\}$
7. $E_{total} = \sum_{i=0}^{R-1} (E_T(i,i+1) + E_R(i,i+1))$
8. $E_t = \frac{E_r . S_d}{\varphi}$
9. $path = \arg_{\min}\left(\sum_{i=0}^{\eta} E_{t,i}\right)$
End
```

The operations involved in above mentioned algorithm ensures that it is capable of exploring and establishing stabilized link irrespective of any number of nodes moving out or moving in a particular domain. In this respect, the proposed algorithm provides full-fledge of scalable features for better path establishment (or inter-domain routing) in presence of variable degree of heterogeneity.

ii) Algorithm Implementation for Ensuring Interoperability

Algorithm incorporates a gateway node (g_{node}). The entire process of data transformation takes place over respective g_{node} itself in particular domain Δ. The algorithm initially considers a specific number of domain Δ which is restricted till the m numbers such that m is much less than total number of mobile nodes (Line-2). Each domain is considered to possess a single g_{node} (Line-4). The algorithm assumes utilizing specific number of routing protocols where the entire communication vector has to pass via g_{node} itself. Any request for data forwarding has to be forwarded to g_{node} which posses direct access to the nodes position and other information too (e.g. energy, buffer, position, etc). The g_{node} after receiving the request from a node within its transmission territory has to look for its nearest neighbor, who happens to be another g_{node} of another domain. For easier in computation, the proposed study considers auto-synchronous operation among all the g_{node} takes place after a periodic time interval. Hence, the process works well with large network with high density. It will also mean that more the communication occurs among the gateway nodes, faster the response time could be.

Now it is essential to understand the transformation scheme adopted by gateway nodes in each domain. Considering that each gateway to be auto-synchronized, all the routing-based queries are processed via gateway node itself. The system can transform for on-demand (Line-6-7) as well as for table-driven (Line-9) routing in heterogeneous MANET system. The on-demand routing protocols are processed using simple search-based mechanism carried out from one to another g_{node} until it finds the destination node. Line-6 shows a special control message *od_msg* is being formed by the gateway node which consists of originator node and destination node address with other respective information fields (e.g. hop counts, sequence number, CRC, flag etc). In order to cater up the demands of the table-driven protocol, each nodes share their respective routing information with each other using *td_msg*. The process also entails g_{node} to perform this address sharing charecteristics only among the communicating nodes. Hence, once the g_{node} receives a request of packet forwarding, it searches for respective domain which either has the destination node or leads to destination node. In any cases, all the addresses of the intermediate nodes are extracted by the respective g_{node} under each domain and are mutually exchange among each other. Once the exchange operation is over, the shortest path among the nodes (with exchanged addressed) are used for transferring the data packets.

Algorithm for Ensuring Interoperability

Input: g_{node} (gateway node), Δ (domain), *n* (total mobile nodes)

Output: Path Establishment.

```
Start
1. Init $g_{node}$, $\Delta$
2. $\Delta \rightarrow [\Delta_1, \Delta_2, \Delta_3, . . . , \Delta_m]$ m<<n
3. $\Delta_i \leftarrow n_p$ && $\Delta_j \leftarrow n_q$
4. Alloc $g_{node} \rightarrow$ single($\Delta$)
5. For $\Delta$=1:m
6. If network is on-demand
7.     $g_{node} \rightarrow$ od_msg($g_{node}(\Delta_j)$)
8. or else
9.     $g_{node} \rightarrow$ td_msg(add(gnode$_{(\Delta j)}$))
10. count++
11. Establish path
End
```

The preliminary steps of the algorithm are more inclined towards appropriate formation of domains and gateway. The technique also considered a decentralized mechanism where the identification of the routing protocol and respective way to transforming it. The proposed system forwards the beacons for collecting the respective information about the mobile nodes and also exchanges the beacons with different gateway nodes, thereby ensuring better interoperability.

iii) Algorithm Implementation for Ensuring Security

The prime purpose of this algorithm is to ensure that any message that is generated from different domains should be authenticated properly. The sole motive of this algorithm is to ensure that it doesn't use iterative nature of encryption and thereby formulate a simple and lightweight security algorithm to ensure privacy, integrity, and non-repudiation. The steps of the algorithm are discussed below:

Algorithm

Input: val_msg (message used for validating), k_{sh} (shared key), IGP_msg (message for on-demand transformation), add_req (message for table-driven transformation)

Output:

```
Start
1. init val_msg, $k_{sh}$
2. $\theta$=val_msg[$k_{sh}$( od_msg, td_msg)]
3. $\theta_1$= $\theta$ o [val_msg[$k_{sh}$, (IGP_msg, add_req)]]
4. val_msg [$k_{sh}$, ( IGP_msg, add_req)], $n_{i-1}$=PRNG
[(IGP_msg, add_req), $k_{s \rightarrow d}$, $n_{i-1}$]
End
```

The operation of the proposed security algorithm is as follows: the source node generates a test message called as *val_msg*, which is required to testify the message validity. This message consists of a shared secret key k_{sh} and message (Line-2). The message in this case could be either *od_msg* for processing on-demand routing or *td_msg* for processing table-driven routing or both. Therefore, the source node forwards the index θ and message. After receiving the *val_msg*, the node (intermediate or destination) performs computation of index θ_1 (Line-3). However, depending upon the situation, the algorithm performs multiple forms of sequential mathematical operations represented by *o* symbol in Line-3. Initially, the system carry out XOR operation which leads to formation of θ.(XOR).val_msg[$k_{s \rightarrow d}$, (IGP_msg, add_req)]. The generated outcome is further overwritten with val_msg

[[$k_{s \to d}$, (IGP_msg, add_req)]]. The generated outcome is further encoded with index θ. Hence, there are only three stages of encryption. The algorithm considers that a malicious node will not attempt to change the index in order to escape the route authentication scheme. In this case, the index will be as it is just to save resources by the malicious nodes. Hence, if the index value is not change, the proposed algorithm considers that there is a presence of malicious / selfish node and thereby access will be denied for forwarding any sorts of data packet forwarding request.

VI. RESULT DISCUSSION

The evaluation of the study was carried out using mobile nodes distributed over multiple domains with one gateway at each domain. The velocity of the mobile nodes differs from 0-20 meter per second. The outcome of is evaluated for overall energy consumption, average end-to-end delay, and throughput. For better benchmarking purpose, the outcome is compared with the most standard work done in relevant topic till date i.e. IDRM [21], CIDR [22], and BGP-Mx [23].

Analysis of Energy Consumption

The outcomes shown in Figure 4 highlights that CIDR extensively dissipates more amount of energy in comparison to other. CIDR uses fisheye algorithm which has higher dependencies on processor power and memory leading to less interoperable as well as less scalable. This also negatively affects the security features if newly added to CIDR (as CIDR doesn't have any security incorporations). Dependency on more memory will also lead to more delay that leads CIDR more prone to traffic jamming attack e.g. DoS. IDRM has better score of energy efficiency as both gateway and non-gateway nodes are configured to forward the data for inter-domain nodes. It is also capable of addressing dynamic topological changes in domain. But unfortunately, this is also one of the limiting factors of IDRM as there are too many of the communication vectors found from almost all the node in bidirectional pattern. This leads to certain level of energy dissipation. This limitation is found to be better addressed by BGP-Mx as it has better supportability of mobility extension and it is also capable of faster discovery process of gateway node.

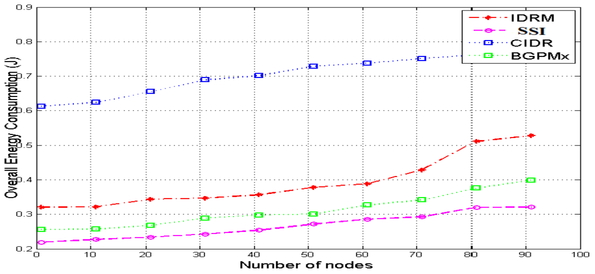

Fig.4: Analysis of Energy Consumption

However, SSI is found with better performance from other existing standards in energy parameter. The prime reason is SSI uses only one gateway which handles multiple requests from many intra-nodes leading to lowering of energy from the intra-nodes. In existing system, the mechanism is always bidirectional in nature between gateway node and intra-node just in route request stage, which is cut shorted as it is assumed that all the gateways are auto-synchronized leading to almost zero retransmission or rebroadcasting of any queries. of their nature of routing) with almost no load on intra-node to perform any sorts of authentication.

Analysis of Average End-to-End Delay

The outcome shown in Figure.5 shows higher end-to-end delay for CIDR as well as IDRM as compared to SSI and BGP-Mx with increasing data size Both CIDR and IDRM leads to more travel time as it will need to broadcast domain membership data. Hence, in case of large network, this delay exponentially increases. CIDR and IDRM does not support dynamic discovery process leading to more time consumption for data transmission. Hence, CIDR and IDRM eventually don't have much better and faster scalable and interoperable features. On the other hand, BGP-Mx has higher supportability of both internal and external dynamic discovery followed by optimization principle thereby reducing the delay to a large extent compared to IDRM and CIDR. However, SSI uses better interoperability approach using distributed data transformation scheme and spontaneous update of gateway node leading to superiorly minimizing the delay. This has also got advantage in security features too. Lower delay in SSI will be quite vigilant over DoS attack.

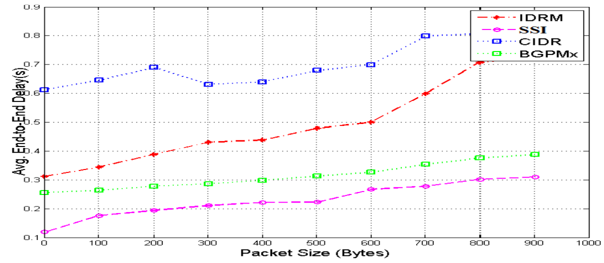

Fig.5: Average End-to-End Delay

Analysis of Throughput

The reason for poor performance of throughput shown in figure 6 for CIDR is its dependency to use bloom filter and iterative hash function. The technique engages enough resources (especially memory) while performing membership management leading to very lower throughput values. Even after increasing mobility, it doesn't increase its throughput. Nearly similar trend is also found for BGP-Mx (although it is slightly better than CIDR). The prime reason for trend of BGP-Mx is basically its route optimization policy which can support on-demand routing but not for table-driven routing scheme.

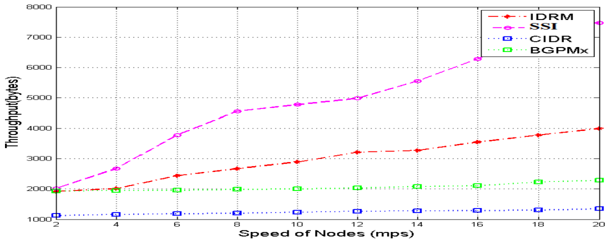

Fig.6: Analysis of Throughput

Table 1 outlines the contribution of the proposed SSI over existing techniques.

Table 1: Summarization of Comparative Performance Outcome

Factor	SSI	CIDR	IDRM	BGPMx
Scalability	Very High	Very Low	Medium	High
Interoperability	Very High	Very Low	Medium	High
Security	Very High	Medium	Low	Low

VII. CONCLUSION

The area of mobile adhoc network is already flooded with various unsolved issues of routing, energy, security, resource allocation etc. None of these problems has been overcome fully although there are large numbers of literatures present to claim it. The existing literature towards MANET is quite symptomatic, which means if it addresses security, it doesn't address much into other problem at same time. This problem becomes much worst when heterogeneous MANET is considered. There are some standard studies being done on this e.g. IDRM, CIDR, BGP-MX etc at present, but none of this addresses security, scalability, and interoperability altogether. The outcome eventually shows better performance with respect to communication performance.

REFERENCES

[1] Pattnaik, P. Kumar, Mall, Rajib, Fundamentals Of Mobile Computing, Second Edition, PHI Learning Pvt. Ltd.,2015

[2] S. V. Bostjancic Rakas and V. V. Timcenko, "Quality of service and security issues in MANET environment," *IEEE-Telecommunications Forum Telfor* (TELFOR), pp. 419-422., 2014

[3] J. Loo, J. L. Mauri, J. H. Ortiz, "Mobile Ad Hoc Networks: Current Status and Future Trends", CRC Press, 2016

[4] Pierre, Samuel, "Next Generation Mobile Networks and Ubiquitous Computing", Idea Group Inc, 2010

[5] H. Hassan, P. Trwoga, I. Kale, "IF-MANET: Interoperable Framework for Mobile Ad Hoc Networks", *Springer- Communications in Computer and Information Science*, pp 54-68, vol.522, 2015

[6] B. Rekha, D.V. Ashoka, "An Enhanced Inter-Domain Communication among MANETs through selected Gateways", *International Journal on Recent Trends in Engineering and Technology*, Vol. 9, No. 1, July 2013

[7] L. Wu, Y. Zhong, W. Zhang, "*Scalable Transmission over Heterogeneous Network: A Stochastic Geometry Analysis*", *IEEE Transactions on Vehicular Technology*, Iss.99, 2016

[8] G. Comarela, G. Gursun, M. Crovella, "Studying Interdomain Routing over Long Timescales", *ACM-Proceedings of the 2013 conference on Internet measurement conference*, pp.227-234, 2013

[9] U. Javed, I. Cunha, D. R. Choffnes, "PoiRoot: Investigating the Root Cause of Interdomain Path Changes", *Proceedings of the ACM SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, pp.183-194, 2013

[10] B. H. Khudayer, M. M. Kadhum, "Reliability of Dynamic Source Routing in Heterogeneous Scalable Mobile Ad Hoc Networks", *IEEE International Conference on Communication, Networks, and Satellite*, pp.71-79, 2014

[11] J. Pan, R. Jain, S. Paul, "Enhanced Evaluation of the Interdomain Routing System for Balanced Routing Scalability and New Internet Architecture Deployments", *IEEE Systems Journal*, Vol.9 , Iss.3, pp.892-903, 2013

[12] Elmokashfi, A. Kvalbein, C. Dovrolis, "SIMROT: A Scalable Interdomain Routing Toolbox", *ACM SIGMETRICS performance evaluation review - special issue on ifip performance*, Vol.39, Iss.2, pp.4-13, 2011

[13] F. Dressler, R. Koch, and M. Gerla, "Path Heuristics using ACO for Inter-Domain Routing in Mobile Ad Hoc and Sensor Networks", *Springer- Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp 128-142, vol.87, 2010

[14] S-H Lee, S. H.Y. Wong, C-K Chau, "InterMR: Inter-MANET Routing in Heterogeneous MANETs", *The 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems*, pp.372-381, 2010

[15] B-Q Han, G-F Feng, and Y-F Chen, "Heterogeneous Resource Allocation Algorithm for Ad Hoc Networks with Utility Fairness", *Hindawi Publishing Corporation International Journal of Distributed Sensor Networks*, Article ID 686189, 13 pages, 2015

[16] Durresia, P. Zhanga, M. Durresia, and L. Barollib, “Architecture for mobile Heterogeneous Multi Domain networks”, *Mobile Information Systems*, vol.6, pp.49–63, 2010

[17] D. Natarajan and A. P Rajendran, “AOLSR: hybrid ad hoc routing protocol based on a modified Dijkstra's algorithm”, *Springer- EURASIP Journal on Wireless Communications and Networking*, vol.90, 2014

[18] K. Zhu, B. Zhou, X. Fu, M. Gerla, “Geo-assisted Multicast Inter-Domain Routing (GMIDR) Protocol for MANETs”, *IEEE International Conference on Communications*, pp.1-5, 2011

[19] E. Souto, R. Aschoff, J. L. Junior, “HTR: a framework for interconnecting wireless heterogeneous devices”, *IEEE Consumer Communication and Networking Conference*, pp.645-649, 2012

[20] R. K. Saluja & R. Shrivastava, “A Scenario Based , Approach For Gateway Discovery Using Manet Routing Protocol” *International Conference on Computer Communication and Informatics*, 2012,

[21] C-K Chau, J Crowcroft, K-W Lee, S H.Y. Wong, “IDRM: Inter-Domain Routing Protocol for Mobile Ad Hoc Networks”, Technical Report of University of Cambridge, Np.708, 2008

[22] B. Zhou, Z. Cao, M. Gerla, “Cluster-based Inter-domain Routing (CIDR) Protocol for MANETs” *IEEE Wireless On-Demand Network Systems and Services*, pp. 19-26, 2009

[23] M. Kaddoura, B. Trent and Ranga, G. Hadynski, “BGP-MX: Border Gateway Protocol with Mobility Extensions”, *IEEE- Military Communications Conference* , pp.687-692, 2011