International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 6, June 2016

A Defense Mechanism for Secure Data Transmission in Mobile ADHOC Networks

[1]R.Kathiroli, [2]N.Niveditha, [3] V.B.Shrinithi, [4] S.Priyanka
[1], [2], [3], [4] Madras Institute of Technology, Anna University, Chennai

***Abstract* - MANET is a self configuring dynamic infrastructure-less wireless network of mobile nodes. The usage of MANET has increased over the past due its ability to form a network anywhere anytime. In addition to such advantages, the cons also follow because of its conditions like remote distribution and its dynamic link changes between nodes. The above stated conditions allow external or internal intruders to create attacks that is passive or active which degrades the efficiency of data transmission. The objective of this paper is to monitor the network activities and detect the presence of any intrusions of attackers. Once a malicious behaviour is noticed, it is ensured that it doesn't participate in the data transmission in the next routine. The addressed attacks are periodic dropping of data packets, periodic delaying of data packets and data packets reordering. We propose a novel algorithm to detect the attacker node and appoint a defense mechanism to isolate such attackers from taking part in the network activities and henceforth increasing the throughput.**

***Index Terms*— Data delay, Data drop, Data reordering, Intrusion, Remote distribution.**

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a collection of mobile nodes forming an ad-hoc network without any central authority to facilitate routing in the network. Each node acts as host and router with limited resources and security. Fig.1. shows the sketch of a mobile ad-hoc network. MANET applications are increasing as they provide the unique ability to form a network anywhere and anytime. Critical situations such as disaster recovery and military operations use MANETs to exchange information. The integrity of data transmission depends on the cooperation of nodes during packet forwarding from the source node to the destined node through intermediate nodes. Remote distribution and open medium of MANETs makes the network more vulnerable to both internal and external attacks. Formation and maintenance of network is difficult owing to the dynamic topology of MANET. To overcome the above mentioned challenges, various security mechanism such as trust calculation [1], initializing incentives [3], and inducing third party like the watchdog for monitoring the network activities [2] have been proposed over the years.

Existing trust management systems [1] use trust values that is comprised of direct trust values based on positive and negative interactions between two nodes, indirect trust values based on recommendations from neighboring nodes. Recommendations help the nodes to decide an optimum and secure route for data transmission. The trustworthy intermediate nodes reduce the probability of internal attacks in MANETs. The external attacks require a defense mechanism to detect the intruder and thereby analyze its impact on the network performance. The detection and exclusion of the intruders is the best approach to remove malicious nodes from the network. Existing detection mechanisms [2], [3] either monitor the intruders or incentivize the participation of trustworthy nodes in the network. But the colluding nodes in the network can disrupt these mechanisms by injecting false detections. This paper introduces a new scheme for securing data transmission by introducing a defense mechanism that integrates the trust management of the nodes in the network with the attack detection model of MANET.

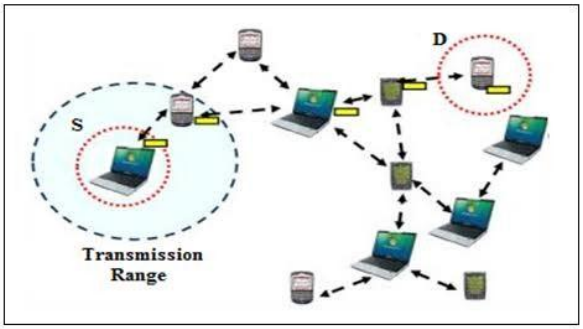

Figure.1. A Mobile Ad-hoc Network Environment

II. RELATED WORK

In the recent year's security in MANETs have been a greater concern, and many defense models have

been proposed against attacks like blackhole in [10] and jelly fish attack in [9]. The main goal is to provide secure wireless network by successful data transmission between two nodes without any malicious intervention of illegitimate nodes that degrades the network performance. These illegitimate nodes are identified through a trust model where nodes with low trust values are considered as probable attackers. The various trust evaluation mechanisms [1], [5], [7], [8], use direct observations and recommendations from neighbour nodes to enhance security in the network.

Shabut et al. [1] proposed a recommendation based trust model with a defense scheme, which utilizes clustering technique to dynamically filter out attacks related to dishonest recommendations, based on number of interactions, compatibility of information and closeness between the nodes. One of the factors leading to dishonest recommendations is selfishness of the nodes which is not addressed in [1]. The selfish nodes tend to preserve their resources by not participating in the network activities.

In [2], Orallo et al. proposed a collaborative approach based on the diffusion of local selfish nodes awareness when a contact occurs, so that information about selfish nodes is quickly propagated. However this collaboration becomes effective only on the proper combination of local and global ratings. The countermeasures for selfish nodes are reputation systems and price systems. The existing methods are inefficient as they exacerbate the already scarce resources problem in MANETs.

Colluding nodes can hack the entire reputation system by providing false or misreported information about other nodes. A hierarchical Account aided Reputation Management system (ARM) provides effective cooperation incentives [3]. The ARM maintains a locality aware distributed hash table that integrates resource and price systems by enabling higher-reputed nodes to pay less for their received services.

Attacks in MANET are inevitable due to the vulnerabilities in the network. Despite the security mechanisms devised to secure the routing path between source and destination nodes malicious activities are induced within the network. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET. The selfish and non-cooperative nodes in the network may refuse to take part in the forwarding process or drops the packets intentionally in order to conserve the resources. These attacks exploit the routing protocol to their own advantage. Packet dropping is one of the main attacks by selfish node which leads to congestion in network by retransmitting control requests. An attacker suppresses or modifies packets originating from few nodes, while leaving the data from the other nodes unaffected, which limits the suspicion of its wrongdoing.

Jelly fish attack is a variant of the denial of service attack and also a type of passive attack which is difficult to detect. It produces delay before the transmission and reception of data packets in the network [4]. Samad et al. identified that defense mechanisms proposed in [3] are targeting closed-loop flows such as TCP that are responsive to network conditions like delay and packet losses and can easily partition the network. In [9] a security scheme called JAM (Jellyfish Attacks Mitigator) is introduced which can be used to detect and mitigate Jellyfish attacks in ad hoc networks. Since Jellyfish attack is passive, it is very strenuous to detect its presence. Henceforth, we propose a defense mechanism that detects the variants of Jellyfish attack. Trust plays a major node in building channels for communication.

Highly Reputed Authenticated Routing (HRARAN) protocol uses reputation and public key cryptographic mechanism to find whether a node is cooperative or compromised in the network [5]. Trust is a very complex concept considering its dynamic nature with the varying interactions between the nodes. A friendship based trust model [8] represents trust as multiple degrees of friendship over time. It uses two metrics to measure friendship namely honesty and confidence. Honesty measures positive and negative behaviours and confidence measures the ability of nodes to provide correct information about other nodes. The model overcomes the limitation of neglecting the social behaviours of nodes when evaluating trustworthiness.

III. PROPOSED WORK

We propose a defense model that ensures secure data transmission between the source and destination by including trustworthy nodes in the path of communication. A recommendation based opinion value estimation model calculates the opinion that each node weighs.

A. System Model:

A MANET topology is considered as G= {V,L} where V={v_1,v_2,….v_n} is the set of nodes and L={l_1,l_2,….l_n} is the set of links in the network. The link between any two nodes is considered to be active when they are in each other's transmission range. At any instant, a multihop MANET has k different routes between source to destination. Our proposed defense system model eliminates untrustworthy nodes and assures that the route with maximum trustworthy nodes is selected. Let M={m_1,m_2,m_3,…..m_n} represent a set of malicious nodes in the network. An attack is said to take place at any given time when M≠ø. Any node found to be causing packet delay, dropping and reordering attack is named as JF-node. Once a JF-node becomes an intermediate node on a selected route, it launches a JellyFish attack variant to degrade the network performance.

B. Opinion Value Estimation:

The estimation model has two components: Direct opinion value and indirect opinion value. Direct opinion value component obtains opinion value from two nodes that have already interacted with each other over a period of time. Direct opinion value is invulnerable to dishonest recommendations and hence it has more weight in opinion value estimation. Fig.2. shows a MANET topology with source node i, destination node j and intermediate nodes m, k. Direct opinion value $\boldsymbol{OP_d}$ of node i about node j is calculated as

$$OP_d = \frac{\alpha_{ij}}{\alpha_{ij} + \beta_{ij}}$$

where α_{ij} - positive interactions between nodes i and j

β_{ij} - negative interactions between nodes i and j

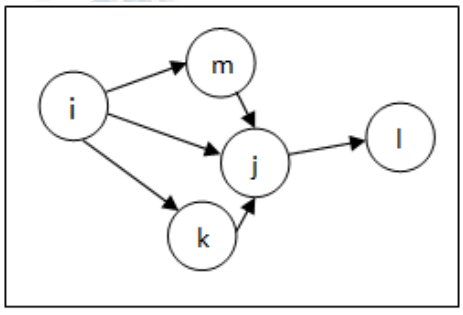

Figure.2. A Manet topology

Indirect opinion value is considered when two nodes have not established any previous interactions through any form of communication. Indirect opinion value is second hand information about direct opinion value between two nodes. Recommendation manager is an intermediate component used in the calculation of indirect opinion value. These recommendations from the intermediate nodes m, k are aggregated to calculate indirect opinion value.

Indirect opinion value of node i about node j with intermediate node m, k is formulated as OP_{id} by calculating the confidence value C_{kj} and recommendation R_{kj}.

$$C_{kj} = 1 - \sqrt{\frac{12\alpha\beta}{(\alpha+\beta+1)(\alpha+\beta)^2}}$$

R_{kj}- second hand direct opinion value

$$OP_{id} = \sum_{k,j=1}^{N} \frac{R_{kj} * C_{kj}}{R_{kj}}$$

Henceforth, the total opinion value of node i on node j is cumulatively formulated as OP_{ij} with weigths 60% on direct opinion value and 40% on indirect opinion as in [3].

$$OP_{ij} = W_d * OP_d + W_{id} * OP_{id}$$

C. Jelly Fish Attack Detection:

We propose an opinion based jellyfish attack detection model as a countermeasure for all three variants of jellyfish attack namely delay, reorder and dropping of packets. Detection and prevention of jelly fish attack is complex due to the compliant nature of the attack with both control and data packets. Due to no functional distinction among mobile nodes in MANETs, any intermediate node can introduce a critical vulnerability. Such JF-nodes alter its forwarding behaviour by delaying or periodic dropping of packets. Consider a scenario as in Fig.3.with node A as source node and node C as destination node. For any data packet D scheduled for transmission between source and destination nodes, intermediate node X performs following steps:

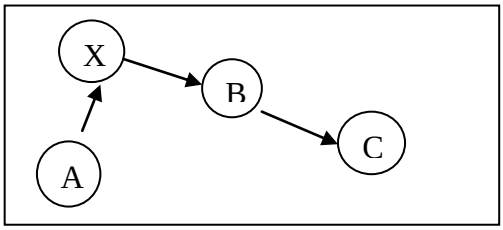

Figure.3. JF attack detection topology

i) . Data Delay Detection:

A node X associates two timers on the successful transmission of a packet to the next immediate hop. The timers are associated with the node for ascertaining the trustworthiness of the nodes of the next immediate hop. Each node calculates forward timer T_f that is required to forward data packets.

$$T_f = T_{process} + T_{queue} + T_{tx}$$

where $T_{Process}$ is the time taken to process the packet, T_{queue} is the time spent by the packet in queue, T_{tx} is the time taken to transmit the data packet.

When node B starts forwarding data to node C, node X associates a primary timer (T_p) at instant t to determine the trustworthiness of the node B.

$$\boldsymbol{T_p\ (t) = T_{EMWA}\ (t) + (\gamma . T_\sigma (t))}$$
$$\boldsymbol{T_{EMWA}\ (t) = (1-\alpha).T_{EMWA}\ (t-1) + \alpha . T_f (t)}$$
$$\boldsymbol{T_\sigma\ (t) = (1-\beta).T_\sigma\ (t-1) - T_f (t)}$$

where $\mathbf{T_{EMWA}}$ is the exponential moving weighted average time, $\mathbf{T_\sigma}$ is the moving average of non-uniform variations between $\mathbf{T_f}$ values. $\boldsymbol{\alpha, \beta}$ and $\boldsymbol{\gamma}$ are the weights chosen from [0,1].

Numerous set of combinations with values of $\mathbf{T_f}$ are simulated in order to choose the primary timer values that adapt to the fluctuations of the dynamic channel. If the node B does not forward the data packets within the time $\mathbf{T_f}$, node X predicts a data delay. Before the expiry of the primary timer if node X hears data packets from node B it does not change the opinion value.

ii). Packet Dropping and Reordering Detection:

After detecting delay in the transmission of data packets, node X sets a secondary timer ($\mathbf{T_s}$) which is equal to half of the primary timer value.

$$\mathbf{T_s = T_p/2}$$

If the node overhears the packet sent within the time $\boldsymbol{T_s}$, it assumes node B to be a delay variance JF-attacker. When the node doesn't overhear the data packet till the expiry of $\boldsymbol{T_s}$, node B is found to drop the data packet.

Reordering of packets occur, if the node X overhears some other data packet other than the current packet. On detecting the jellyfish attacker nodes, the opinion value of these JF nodes is reduced. The nodes for which the opinion value falls below minimum value ($\boldsymbol{OP_{min}}$) are blacklisted.

IV. REVOKING CERTIFICATES:

Certificate Authority (CA) is a third party member that issues information about nodes with revoked certificates in the network at regular intervals. Identified attacker node is withheld from transmitting data for time $\mathbf{T_b}$ (blacklist timer) and a route error (RERR) message is sent to the source. The isolated nodes are re-issued certificates after the expiration of $\mathbf{T_b}$ to prevent false positives. A node blacklisted three times is given no more chance and is blacklisted for the rest of the network lifetime.

V. JELLYFISH ATTACK DETECTION ALGORITHM

Notations:
N: Number of nodes
S, D, k: Source, Destination, Intermediate node
A: Attacker JF-node
ρ: Considered Packet
T_p, T_s: Primary and Secondary timers at n
$OP_n[1..N], 1 \le n \le N$: Set of opinion value for each node
OP_{ij}: Opinion value of i on j.
OP_{min}: Minimum edge for opinion value
S_k^{JF}: Set of identified JF nodes by k
Algorithm:

1. Initialise OP_{max} as 1
2. For i =1 to NN
3. $S_k^{JF} = \emptyset$
4. For j=1 to NN
5. $OP_{ij} = OP_{max}$
6. For each ρ transmitted from X
7. Set T_p, T_s for ρ
8. Forward ρ to A
9. If (T_p is expired) then
10. If (ρ is not overheard by X) then
11. $T_s = T_p/2$
12. If (ρ is not overheard by X) then
13. If (T_s is not expired) then
14. A is a JF-delay Attacker
15. Decrement OP_{XA}
16. Else
17. A is a JF-drop Attacker
18. Decrement OP_{XA}
19. Else
20. If(p′ is overheard by X) then
21. A is a JF-reorder Attacker
22. Decrement OP_{XA}
23. If ($OP_{XA} < OP_{min}$) then
24. $S_k^{JF} = S_k^{JF} \cup \{A\}$

25. X sends RERR to S
26. S reinitiates the routing
27. End

VI. SIMULATION RESULTS

In this section, we evaluate effectiveness of the proposed JellyFish attack detection algorithm for identifying JF-nodes through simulation process. Improvement in TCP throughput once a JF-node is detected and blacklisted by the proposed countermeasure method, is a measure of effectiveness of the proposal. The simulation is conducted using NS2 simulator, an open source discrete event simulator designed to support research in computer networking.

Fig.4. shows TCP client throughput before and after detection of attacker nodes by applying the defense mechanism. As depicted in the figure, the proposed detection method identifies JF-node(s) and increases the network throughput by preventing their participation in route discovery process. The detection process is not significantly affected by number of attackers as it identifies all JF-nodes en route. Jelly Fish attack, however, may not be launched by all JF-nodes at same time. As detection happens only after an attack is initiated and discovered by a neighbor, throughput shows slight decrease with increase of number of attackers. This decrease is due to time taken to detect all the JF-nodes in the network. This time, called 'initial detection period', depends on the number of JF-nodes, time at which an attack is initiated by a node and network topology.

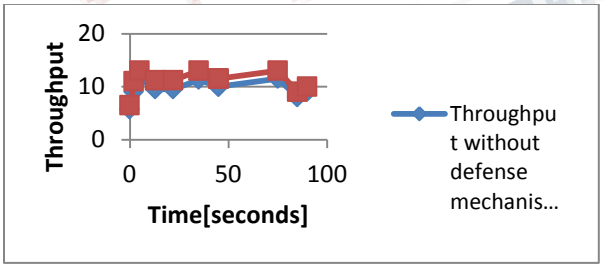

Figure.4. Throughput analysis of network with and without attacker nodes

Fig.5. shows the effect of Jellyfish attack detection algorithm on end-to-end delay in presence of varying number of JF-nodes. With increase in JF-nodes, delay increases gradually. Fluctuations in the delay with increasing number of JF-nodes is the result of (a) the network mobility, (b) random timings of attacks, (c) participation of random number of JF-nodes in a given simulation run (d) all JF-nodes may not be en-route. As JF-nodes may be spanned across multiple routes, detection may take longer time.

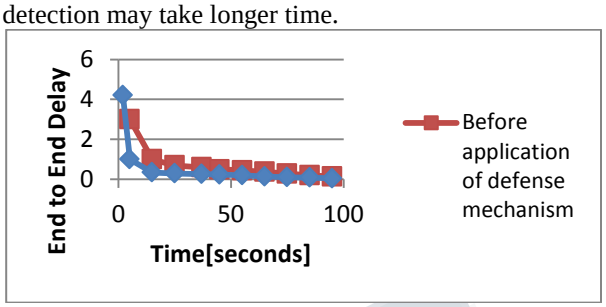

Figure.5. Average end to end delay analysis of network with and without attacker nodes

Fig.6. shows the overhead increase when there are malicious nodes in the network. The TCP control overhead is found to be low when malicious activities are not present in the network environment. Based on simulation results generated over various MANET scenarios with varying number of attackers and attack parameters, it has been observed that Jellyfish attack causes network performance degradation in terms of network throughput, end to end delay and control overhead. It is seen during evaluation process that the placement and number of attackers with respect to the selected route for data communication greatly affect the underlying network performance. The protocol compliant nature of JF-attack makes its detection process a difficult task.

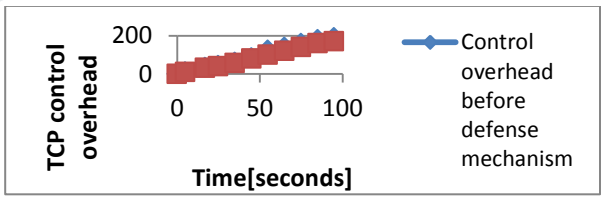

Figure.4. Control overhead analysis of network with and without attacker nodes

VII. CONCLUSION

The objective of the paper is accomplished by reducing the effect of passive attacks such as periodic data delaying, data dropping and data packet reordering. The proposed defense mechanism detects the intrusion of the attacker nodes and reduces the trustworthiness of the attacker node, thereby deterring its participation in data transmission of the network. The proposed model is tested by extensive simulation in terms of increased

throughput; reduced end to end delay also false positives are reduced by giving a second chance to attacker nodes to participate in the data transmission of the network. The security in the network can be improvised by integrating the defense mechanisms of similar other attacks that forbid the legitimate nodes in the network or degrade the throughput of the network.

REFERENCES

[1] A.M. Shabut, K.P Daha, S.K. Bista, and I.U. Awan, "Recom-mendation-based Trust Model with An Effective Defence Scheme for MANET," IEEE Trans. on Mobile Computing, vol. 14, no. 10, pp.2102-2115, Oct. 2015.

[2] E.H. Orallo, M.D. Olmos, J.C. Cano, C.T. Calafate, and P. Manzoni, "CoCoWa: A Collaborative Contact-Based Watchdog for Detecting Selfish Nodes," IEEE Trans. on Mobile Computing, vol. 14, no. 6, pp. 1162-1175, June 2015.

[3] H. Shen, and Z. Li, "A Hierarchical Account-Aided Reputation Management System for MANETs," IEEE/ACM Trans. on Networking, vol. 23, no. 1, pp. 70-84, Feb. 2015.

[4] V. Laxmi, C. Lal, M.S. Gaur, and D. Mehta, "JellyFish Attack: Analysis, Detection and Countermeasure in TCP-based MANET," Elsevier Ltd, vol. 22, pp. 99–112, June 2015.

[5] P. Annadurai, and S. Vijayalakshmi, "Highly Reputed Authenticated Routing in MANET(HRARAN) ," Springer, vol. 83, no. 1, pp. 452-475, Feb. 2015.

[6] W. Liu, H. Nishiyama, N. Ansari, J. Yang, and N. Kato, "Cluster-based Certificate Revocation with Vindication Capability for Mobile Ad-Hoc Networks," IEEE Trans. on Parallel and Distributed Systems, vol. 24, no. 2, pp. 239-249, Feb. 2013.

[7] U. Venkanna, A. Leela, and R. Velusamy, "A Cooperative Routing for MANET-based on Distributed Trust and Energy Management," Springer Wireless Personal Communications, vol. 81, no. 3, pp. 962-979, Nov. 2014.

[8] A.M. Shabut, K. Dahal, and I. Awan, "'Friendship-based Trust Model to Secure Routing Protocols in Mobile Ad-Hoc Networks," IEEE Conference on Future IoT &Clous, Aug. 2014.

[9] Fahad Samad, Qassem Abu Ahmed, Asadullah Shaikh, Abdul Aziz, "JAM: Mitigating Jellyfish Attacks in Wireless Ad-Hoc Network," Springer Wireless Networks, vol. 281, pp. 432-444, March 2012.

[10] A. Mishra, R. Jaiswal, and S. Sharma, "A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad-Hoc Network," Advance Computing Conference (IACC), IEEE 3rd International, pp. 499-504, Feb. 2013.

[11] Z.J. Haas, "The New Routing Protocol for The Reconfigurable Wireless Networks," Proceedings of International Universal Personal Communications, vol. 2, pp. 562-566, Oct. 1997.

[12] A. Iwata, C.C. Chiang, G. Pei, M. Gerla, and T.W. Chen, "Scalable Routing Strategies for Ad-Hoc Wireless Networks," IEEE Journal on Selected Areas in Communications, vol. 17, no. 8, pp. 1369-1379, Aug. 1999.

[13] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol for Ad-Hoc Networks," Proceedings of Conference on Multi Topic, pp. 62-68, 2001.

[14] M. Joa-Ng, and I.T. Lu, "A Peer-To-Peer Zone-based Two-Level Link State Routing for Mobile Ad-Hoc Networks," IEEE Journal on Selected Areas in Communication, vol. 17, no. 8, pp. 1415-1425, Aug. 1999.

[15] D.B. Johnson and D.A. Maltz, "Dynamic Source Routing in Ad-Hoc Wireless," Journal of Mobile Computing, vol. 353, pp. 153-181, 1996.

[16] A. Khannous, A. Rghioui, F. Elouaai, and M. Bouh-orma, "MANET Security: An Intrusion Detection System-based on The Combination of Negative Selection and Danger Theory Concepts," Proceedings Of Fifth International Conference on Next Generation Networks and Services, pp. 88-91, May 2014.

[17] W. Liu, H. Nishiyama, N. Ansari, J. Yang, and N. Kato, "Cluster-based Certificate Revocation with Vindication Capability for Mobile Ad -Hoc Networks," IEEE Trans. on Parallel and Distributed Systems, vol. 24, no. 2, pp. 239-249, Feb. 2013.

[18] N. Mohammed, H. Otrok, L. Wang, M. Deb-babi, and P. Bhatta-charya, "Mechanism Design-based

Secure Leader Election Model for Intrusion Detection in Manet," IEEE Trans. on Dependable and Secure Computing, vol. 8, no. 1, pp. 89-103, Jan.-Feb. 2011.

[19] C.S.R. Murthy, and B.S. Manoj, "Ad-Hoc Wireless Networks Architectures and Protocols," Dorling Kindersley India Pvt. Ltd., India, 2006.

[20] S. Murthy, and J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks," Jounal of Mobile Networks and Applications, vol. 1, no. 2, pp. 183-197, June 1996.

[21] V.D. Park, and M.S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proceedings of Sixteenth Annual Conference on Driving The Information Revolution, vol. 3, pp. 1405-1413, April 1997.

[22] G. Pei, M. Gerla, and T. Chen, "Fisheye State Routing:A Routing Scheme for Ad-Hoc Wireless Networks," International conference on communications, vol. 1, pp. 70-74, 2000.

[23] C.E. Perkins, and P. Bhagwat, "Highly Dynamic Destination Sequenced Distance Vector Routing (DSDV) for Mobile Computers," Proceedings of Conference on Communications Architectures, Protocols and Applications, pp. 234-244, Oct. 1994.

[24] C.E. Perkins, and E.M. Royer, "Adhoc On-Demand Distance Vector Routing," Proceedings of Workshop on Mobile Computing Systems and Applications, pp.90-100, Feb. 1999.

[25] V. Raychoudhury, J. Cao, R. Niyogi, W. Wu, and Y. Lai, "Top K-Leader Election in Mobile Ad-Hoc Networks," Journal of Pervasive and Mobile Computing, vol. 5, no. 22, pp. 181-202, Jan. 2013.