International Journal of Engineering & Technology, 7 (4) (2018) 5940-5944

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.22845
Research paper

A novel cluster-based traffic analysis using trust computation in mobile ad hoc network

T. Dheepak [1] *, S. Neduncheliyan [2]

[1] *Research Scholar, Department of Computer Science, Research & Development Centre, Bharathiar University Coimbatore, Tamil Nadu, India*
[2] *Dean, School of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Selaiyur, Chennai, Tamilnadu, India*
**Corresponding author E-mail: india.nedun@yahoo.com*

Abstract

Mobile Ad-hoc Network (MANET) is a wireless network which is mobile and is deployed for an immediate or short-term purpose. MANETs operate by sharing information among its neighbors. Every node in a MANET utilizes responsibility for information flow since central coordination is absent. Hence, every node in a MANET completely trusts its neighbors for information distribution. Nodes in a MANET are vulnerable to several security threats which seek to use the weaknesses of the network. In this paper, a novel cluster-based traffic analysis is a reactive on-demand method for secured routing. This proposed methodology explains the method to overcome the traffic in the MANET by using trust-based cluster method.

Keywords: *MANET; Traffic Analysis; Clustering; Trust Calculation; Reactive; on-Demand.*

1. Introduction

In a MANET, nodes collaborate to share data [1]. A node needing to send information transmits the information to its neighbor which like this propagates it to its neighbors until the point when it achieves the required goal. This system puts an innate trust among other nodes in the system for information proliferation. An attacker can exploit this trust relationship among the nodes accordingly trading off the system. Additionally, because of the movement of the nodes and powerfully changing system topology, it is difficult to determine whether a packet is dropped on account of the inherent system qualities or the nearness of an attacker.
Ad Hoc Network works by setting up a natural trust relationship among its taking an interest node. Thus every node in a MANET can work as a switch. Notwithstanding, since the remote medium is shared and there is an absence of focal coordination, impromptu systems are defenseless against assaults from different gadgets inside the transmission run. MANETs confront vulnerabilities as a result of a conventional remote medium, absence of physical security for the mobile nodes, and finish trust among nodes on account of an absence of incorporated primary leadership substance [2] [3]. MANETs are powerless to DoS assaults as they do not have a reasonable line of the guard [4][5]. Impromptu systems work by building up an inborn trust relationship among its taking interest nodes. Henceforth every node in a MANET can work as a switch. Every node in a MANET confides in its neighbors to complete system exercises, for example, packet sending and packet conveyance until the point that every packet achieves the planned goal. Regularly, attackers endeavor to exploit this specific characteristic present in the nodes in a MANET. In this way, overseeing trust likewise turns into a vital issue [6-7].

2. Related works

Qi, Huamei, et al. [8] proposed a clustering calculation take the lingering energy and gathering mobility into thought by limiting least cycle times. Additionally, a circulated blame identification calculation and cluster head reinforcement system are displayed to accomplish the occasional and ongoing topology upkeep to improve the power of the system.
Sugumar, Rajendran, et al. [9] a trust-based validation conspire for group-based VANETs is proposed. The vehicles are clustered, and the trust level of every node is evaluated. The trust degree is a blend of direct trust degree and circuitous trust degree.
Oubabas, Sarah, et al. [10] proposed another methodology that chooses a solid group head dependent on a mixture approach consolidating solidness and trust factors. The creators presented a clock that lessens the control activity amid a grouping procedure by wiping out the opposition of nodes to wind up the cluster head.
Bala, K, et al. [11] proposes a novel system organize information-based control model to distinguish and ease directing assaults. The proposed system utilizes time variation depictions to distinguish steering assaults. Every node learns to arrange points of interest utilizing the system information hypothesis (NIT) to get the learning about the nodes of the system, the neighbor locations, energy subtle elements, relocation speed from the course revelation packets and answer packets.
Zhang, Wei, et al. [12] to take care of the issue of evaluation and vulnerability of trust, a new trust the executive's plot dependent on Dempster-Shafer proof hypothesis for pernicious node recognition has proposed in this paper. Right off the bat, by considering the spatiotemporal relationship of the information gathered in sensor nodes in the neighboring zone, the trust degree can be assessed. Also, as per the D-S hypothesis, the trust show is set up to check

the number of responsible practices of trust, doubt or vulnerability, further to assess the immediate trust esteem and circuitous trust esteem.

3. Proposed cluster-based traffic analysis for mobile ad hoc network

In this proposed method, a novel cluster-based traffic analysis is an on-demand and reactive method for secured routing. It establishes the system into 1-hop disjoint clusters, whereby each node selects its cluster head (CH), which should be 1-hop neighbors, most trustworthy and qualified node. Cluster members in Cluster-based traffic analysis method forward packet only within the trusted CHs. The following steps are involved in the finding of the traffic and malicious node in the network.

Step 1: Cluster Formation: In this method, the formation of the cluster has done by using Cosine Similarity method. This method usually elects cluster-heads (CH) taking into consideration like Speed of the node, Power of a node, Degree Difference and Sum of distances. Using the above metrics, the weight of individual nodes can be a calculation for electing the CH.

Ba_j = Total battery life of a_j

C- Ba_j = Current battery life of a_j

TVa_j = Expected Trust value of a_j (1)

C- TVa_j= Current Trust value of a_j

Da_j = expected 1-hop distance of a_j from the neighboring nodes

C- Da_j = current distance of a_j from the neighboring nodes

R-IHa_j= Required interaction history of a_j with the interaction nodes

C-IH a_j = Current interaction history of a_j with the interaction nodes

Algorithm 1: Cluster Formation Step by Step Procedure
Input: Set of nodes
Output: Set of clusters
Step 1: Begin cluster = 1/* represent cluster number 1*/
Total number of nodes = A
Step 2: For (Number of nodes a_j = 1; number of nodes a_j< A; number of nodes a++)
Step 3: if ((C- Ba_j>=Ba_j) (TVa_j>=C- TVa_j) (C- Da_j>= Da_j) (R-IHa_j>= C-IH a_j)
Node a_j cannot be a part of the cluster formation
Step 4: Else Node a_j can be a part of the cluster formation
Step 5: Repeat
Step 6: Repeat
Step 7: Select a node $a_j$which is 1 hop distance apart from other nodes where
Step 8: Do
Step 9: $A = a_j$; d=d1; $A= \cup_{a_j \in A, a_j \neq a_k} \{a_k | \text{ distance } (a_j, a_k) \leq TRANSa_j\}$
Step 10: Draw a circle with a_j as center and d as a radius
Step 11: Compute new radius (d1) = d+ $|a_j - a_k|$
Step 12: while $a_j \neq a_k$
Step 13: Cluster – 1 is formed with cooperating nodes lying within the circle;
Step 14: End
Step 2: Node Trust Calculation: In this method, the trust value computation depends on the data that every node can associate with another node. Relevant information about other nodes has associated by examining the forwarded packets, overhead packets and received packets, given that proper reinforcements have utilized at various protocol layers. The trust between the two nodes has represented in a 3-dimensional opinion metrics (Acceptance, Rejection and Doubtful).

$$T_j^i = (a_j^i, r_j^i, d_j^i) \text{ such that } a_j^i + r_j^i + d_j^i = 1 \quad (1)$$

T_j^i indicates the node i's evaluation about any node i's trustworthiness
a_j^i indicates the acceptance that i holds for j (i.e., the possibility that a node j can be trusted by node i)
r_j^i indicates the rejection that i holds for j (i.e., the possibility that a node j can't be trusted by i).
d_j^i indicates the doubtful that i holds for j (i.e., doubtful fills the void in the absence of both acceptance and rejection).
In the proposed method, a node observes other nodes' behavior to obtain and store all plus (p) and minus (n) events about their trustworthiness. So, the opinion metrics of T_j^ican be performed as a function of p and n as follows:

$$a_j^i = \frac{p}{p+n+2}$$

$$r_j^i = \frac{n}{p+n+2}$$

$$d_j^i = \frac{2}{p+n+2}$$

Algorithm 2: Cluster Head Selection Step by Step Procedure
Step 1: CHcur← 0
Step 2: CHprev← 0
Step 3: Timeprev← 0
Step 4: now () ← 0
Step 5: Time - Out_{loop}← 3 * COUNTR
Step 6: The trust value can be further evaluated by the above equation (1)
Step 7: Interaction history (IH) ≥ 0
Step 8: while ($Time_{prev}$≤ now ()or TRUST_VALUE (CH_{prev}) ≤ 1 = true)
Step 9: do CH_{prev} remains as a cluster head
Step 10: end while
Step 11: if TRUST_VALUE (CH_{prev}) = TRUST_VALUE (CH_{cur}) and IH (CH_{prev}) = IH (CH_{cur})
Step 12: then both CH_{cur} and CH_{prev} remain as Cluster Heads
Step 13: Else
Step 14: select new CH
Step 15: end if
Step 3: Local Cluster Formation: If the elected CH is a malicious node, then it threatens the network system connectivity. In this proposed method, (which can be identified by the above step) a node should change its CH when it becomes Malicious node to evade the overhead causing by revoking the first step of cluster formation.
Step 4: Handling of Route Request by CH: A CH receives the Route Request from any node in the network. CH will check for the trust value of the node then it will find and compare with the acceptance, rejection and doubtful values. If the rejection value of a node is higher than the given rejection threshold, then that node can be discarded as the Malicious node.
Step 5: Handling of Malicious Nodes: In this method, if any node determines that the next hop in the source route packet be malicious, then it attempts to attain another trustfulness of the intermediary nodes to the next jump in the same route by searching its cache or routing table for the route to the destination.

4. Result and discussion

4.1. Simulation setup

The proposed Cluster based Traffic Analysis method has been simulated in NS-2 software environment. 100 nodes considered as a total number of nodes, the simulation area is (250m X 250m), each initial node energy is 20000 joules, packet size is 512 bytes, the total execution time for simulation is 300 seconds, each node operating power is 10mW, 10%, and 20% are the percentages of the malicious nodes.

4.2. Performance analysis of the proposed method with 10% malicious nodes

Table 1 represents the number of clusters formed by existing clustering method and proposed cluster-based traffic analysis method at 10% malicious nodes. Figure 1 depicts the graphical representation of the number of cluster formation in the existing method and the proposed method. From table 1 and figure 1, the proposed method gives the increased number of clusters than the existing method. The increased number of clusters reduces the packet loss and end to end delay.

Table 1: Number of Clusters Formed by Existing Clustering Method And the Proposed Cluster Based Traffic Analysis Method at 10% Malicious Nodes

Number of Nodes	Number of Clusters formed	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
50	8	9
100	11	12
150	18	20
200	21	22
250	22	23
300	26	27

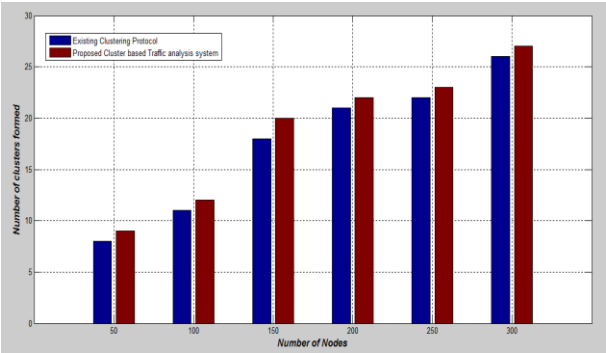

Fig. 1: Number of Clusters Formed Proposed Cluster Based Traffic Analysis Method and the Existing Clustering Method by Many Clusters Formed at 10 % Malicious Nodes.

Table 2 represented the average packet delivery ratio of the existing clustering method and proposed a cluster-based traffic analysis method at 10% malicious nodes. Figure 2 depicts the graphical representation of the average packet delivery ratio in the existing method, and the proposed model. From table 2 and figure 2, the proposed method gives the increased average packet delivery ratio than the existing method.

Table 2: Average Packet Delivery Ratio of the Existing Clustering Method and Proposed Cluster Based Traffic Analysis Method at 10% Malicious Nodes

Number of Nodes	Average Packet Delivery Ratio	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
50	0.9221	0.9396
100	0.8782	0.9842
150	0.8725	0.8862
200	0.8219	0.8457
250	0.7579	0.7863
300	0.6601	0.6883

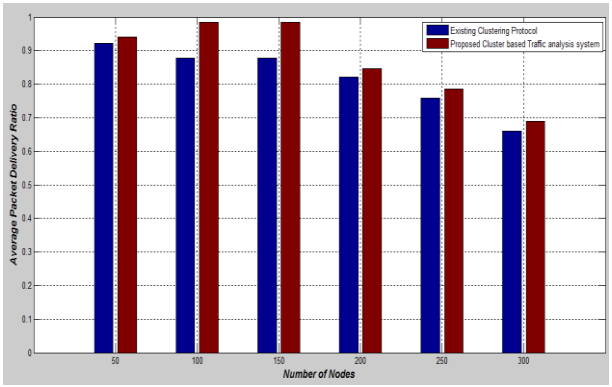

Fig. 2: Graphical Representation of the Average Packet Delivery Ratio of an Existing Clustering Method and the Proposed Cluster Based Traffic Analysis Method at 10% Malicious Nodes.

Table 3 represented the remaining energy consumption in joules of the existing clustering method and proposed a cluster-based traffic analysis method at 10% malicious nodes. Figure 3 depicts the graphical representation of the remaining energy consumption in joules in the existing method and the proposed method. From table 3 and figure 3, the proposed method gives the increased remaining energy consumption (in joules) than the existing method.

Table 3: Remaining Energy Consumption in Joules of the Existing Clustering Method and Proposed Cluster Based Traffic Analysis Method at 10% Malicious Nodes

Number of Rounds	Remaining Energy Computation in Joules	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
0	0.5	0.5
100	0.41	0.45
200	0.24	0.34
300	0.2	0.29
400	0.18	0.27
500	0.12	0.18
600	0	0.10
700	0	0.8
800	0	0

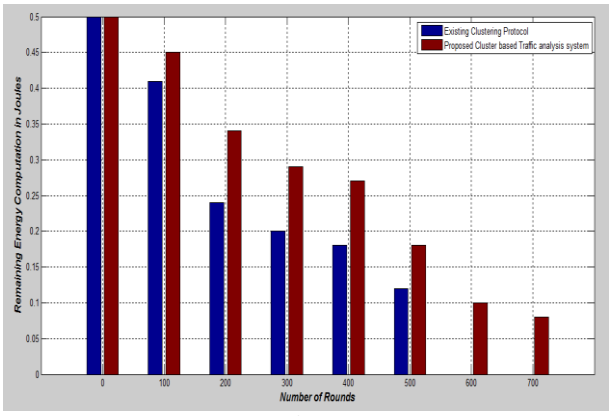

Fig. 3: Graphical Representation of the Remaining Energy Consumption (In Joules) of the Existing Clustering Method And Proposed Cluster Based Traffic Analysis Method at 10% Malicious Nodes

4.3. Performance analysis of the proposed method with 20% malicious nodes

Table 4 represents the number of clusters formed by existing clustering method and proposed cluster-based traffic analysis method at 20% malicious nodes. Figure 4 depicts the graphical representation of the number of cluster formation in the existing method and the proposed method. From table 4 and figure 4, the proposed method gives the increased number of clusters than the existing method. The increased number of clusters reduces the packet loss and end to end delay.

Table 4: Number of Clusters Formed by Existing Clustering Method And The Proposed Cluster Based Traffic Analysis Method at 20% Malicious Nodes

Number of Nodes	Number of Clusters formed	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
50	8	8
100	11	10
150	16	19
200	22	23
250	21	20
300	26	27

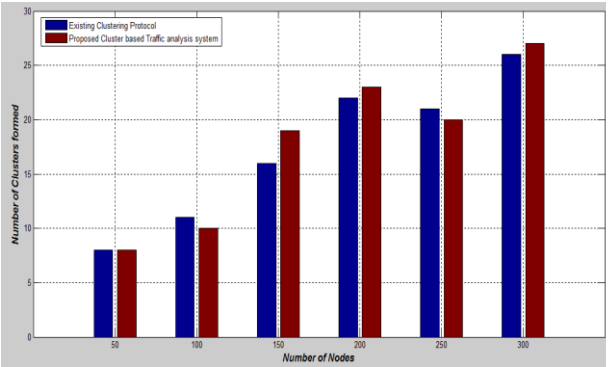

Fig. 4: Graphical Representation of the Number of Clusters Formed Proposed Cluster Based Traffic Analysis Method and the Existing Clustering Method by Many Clusters Formed at 20 % Malicious Nodes.

Table 5 represented the average packet delivery ratio of the existing clustering method and proposed a cluster-based traffic analysis method at 20% malicious nodes. Figure 5 depicts the graphical representation of the average packet delivery ratio in the existing method and the proposed method. From table 5 and figure 5, the proposed method gives the increased average packet delivery ratio than the existing method.

Table 5: Average Packet Delivery Ratio of the Existing Clustering Method and Proposed Cluster Based Traffic Analysis Method at 20% Malicious Nodes

Number of Nodes	Average Packet Delivery Ratio	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
50	0.8427	0.8592
100	0.8165	0.8235
150	0.7858	0.8181
200	0.7406	0.7757
250	0.6776	0.6943
300	0.6113	0.6362

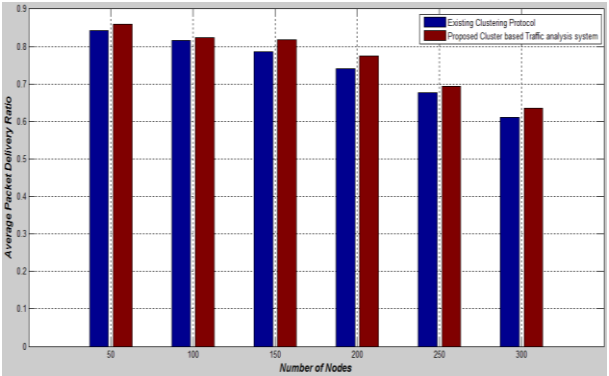

Fig. 5: Graphical Representation of the Average Packet Delivery Ratio of the Existing Clustering Method and the Proposed Cluster Based Traffic Analysis Method at 20% Malicious Nodes.

Table 6 represented the remaining energy consumption in joules of the existing clustering method and proposed a cluster-based traffic analysis method at 20% malicious nodes. Figure 6 depicts the graphical representation of the remaining energy consumption in joules in the existing method and the proposed method. From table 6 and figure 6, the proposed method gives the increased remaining energy consumption (in joules) than the existing method.

Table 6: Remaining Energy Consumption in Joules of the Existing Clustering Method and Proposed Cluster Based Traffic Analysis Method at 20% Malicious Nodes

Number of Rounds	Remaining Energy Computation in Joules	
	Existing Clustering Method	Proposed Cluster based Traffic analysis method
0	0.5	0.5
100	0.35	0.38
200	0.2	0.29
300	0.17	0.24
400	0.15	0.23
500	0.1	0.16
600	0	0.08
700	0	0
800	0	0

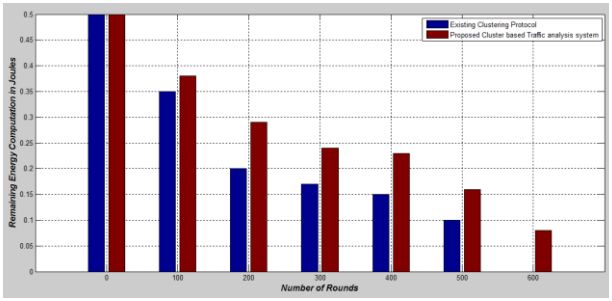

Fig. 6: Graphical Representation of the Remaining Energy Consumption in Joules of the Existing Clustering Method and the Proposed Cluster Based Traffic Analysis Method at 20% Malicious Nodes.

5. Conclusion

In the research work, a novel cluster-based activity examination strategy has proposed to transmit the packet in the far-reaching system and the identification of the malicious node. The trust esteem computation strategy has performed in this procedure, to know the trust of the neighbouring nodes in the system. The malicious node has removed from the network. The packet conveyance proportion, remaining energy utilization in joules are clustered when the number of nodes and additionally the number of malicious nodes exhibited in the system. It builds the lifetime of the system through this technique.

References

[1] Usman, Muhammad, et al. "QASEC: A secured data communication scheme for mobile Ad-hoc networks." *Future Generation Computer Systems* (2018). https://doi.org/10.1016/j.future.2018.05.007.

[2] Sen, Biswaraj, et al. "A Trust-Based Intrusion Detection System for Mitigating Blackhole Attacks in MANET." *Advanced Computational and Communication Paradigms*. Springer, Singapore, 2018. 765-775. https://doi.org/10.1007/978-981-10-8237-5_74.

[3] Liu, Gao, Zheng Yan, and Witold Pedrycz. "Data collection for attack detection and security measurement in mobile ad hoc networks: A survey." *Journal of Network and Computer Applications* (2018). https://doi.org/10.1016/j.jnca.2018.01.004.

[4] Vanamala, C. K., and G. Raghvendra Rao. "SC-MANET: Threats, Risk and Solution Strategies for Security Concerns in Mobile Ad-Hoc Network." *Computer Science Online Conference*. Springer, Cham, 2018. https://doi.org/10.1007/978-3-319-91192-2_30.

[5] Mehra, Ankush. "TO ENHANCE THE SECURITY AND IMPROVE THE PERFORMANCE OF AODV PROTOCOL IN MANET USING DELAY PER HOP TECHNIQUE." *Global Journal of Computers & Technology* 6.2 (2018): 354-365.

[6] Srinivasan, A., and Shaik Naseera. "Trust and location-based service in mobile social networks–A survey." *Multiagent and Grid*

Systems 14.3 (2018): 263-282. https://doi.org/10.3233/MGS-180291.

[7] Borkar, Gautam M., and A. R. Mahajan. "A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks." *Wireless Networks* 23.8 (2017): 2455-2472. https://doi.org/10.1007/s11276-016-1287-y.

[8] Qi, Huamei, et al. "A Robust and Energy-Efficient Weighted Clustering Algorithm on Mobile Ad Hoc Sensor Networks." *Algorithms* 11.8 (2018): 116. https://doi.org/10.3390/a11080116.

[9] Sugumar, Rajendran, Alwar Rengarajan, and Chinnappan Jayakumar. "Trust-based authentication technique for cluster-based vehicular ad hoc networks (VANET)." *Wireless Networks* 24.2 (2018): 373-382. https://doi.org/10.1007/s11276-016-1336-6.

[10] Oubabas, Sarah, et al. "Secure and stable Vehicular Ad Hoc Network clustering algorithm based on hybrid mobility similarities and trust management scheme." *Vehicular Communications* 13 (2018): 128-138. https://doi.org/10.1016/j.vehcom.2018.08.001.

[11] Bala, K., S. Jothi, and A. Chandrasekar. "An enhanced intrusion detection system for mobile ad-hoc network based on traffic analysis." *Cluster Computing* (2018): 1-8. https://doi.org/10.1007/s10586-018-2545-9.

[12] Zhang, Wei, et al. "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks." *The Journal of Supercomputing* 74.4 (2018): 1779-1801. https://doi.org/10.1007/s11227-017-2150-3.