International Journal of IT & Knowledge Management (ISSN: 0973-4414)
Volume 11 • Issue 2 pp. 125-136 Jan 2018 - June 2018 www.csjournals.com

Hybridized ACO and Clone Detection in MANETs

Anubha[1], Dr.RPS Bedi[2]
Research Scholar[1], Joint Registrar[2]
IKG Punjab Technical University, Kapurthala, Punjab

Abstract: A Mobile ad-hoc networks (MANET) is a system of self-organizing mobile nodes that operate without the assistance of centralized administration or planned to achieve. MANETs are especially subject to different security risks as a result of this feature. For interaction in a MANET, various routing systems are designed. Furthermore, since MANETs are broadly used in apps like communication & data sharing, security is a big issue. This paper introduces a novel routing technique for MANETs that uses the Ant Colony Optimization (ACO) method in combination with a Linear programming algorithm to minimize entire system delay. The suggested system was introduced with NS2, and its results are evaluated using the network's remaining energy, packet drops, PDR, throughput, & E2E delay. The test outcomes reveal that the network outperforms towards the existing Methodological approaches.
Keywords: Mobile Ad hoc network (MANET), ACO, Clone node (CN), PEDM, Network Security.

I. INTRODUCTION

MANET has appeared one of the most inventive as well as engaging areas of wireless communication, promising to become more prevalent in our daily lives. MANET's basic structure represents a system that are openly but adaptively self-assemble (i.e., nodes are autonomous) into arbitrary & temporary configurations with no infrastructure support (Conti et al., 2003). When compared to other networking solutions, the benefit of using MANET is that it provides a great deal of freedom at a low cost. Because of the accuracy and convenience with which these systems can be deployed, they are optimal for recovery following a natural or man-made disaster (hurricane, earthquake, flooding, and nuclear explosion), business affiliates exchanging data during a conference, as well as military communicators in a battlefield. One of the most tough tasks that a system designer faces in MANET is determining the best route among communication end-points, which can be challenging dynamic topology. In the existing research, a few routing systems have been suggested. All these, such as DSDV, AODV, DSR, & TORA, have been thoroughly modeled for a variety of situations (Ishu and Ali,2017). Each routing system's optimal goal is to direct traffic from sources to destinations while optimizing system performance and reducing losses. For this article, designers present a different MANET-specific model called on the ACO method (Bansal et al.,2012) as well as its mixture with queuing analysis tools.

The organization of paper is Section II shows the clone detection in MANET & ACO. Section III explains about related work. Section IV explains the suggested approach of work. Section V presents the simulation outcomes & article is concluded in section VI.

II. CLONE DETECTION

The main security issue in MANETs is protecting the internet protocol from malware activity as well as detecting or preventing malicious nodes in the communication system (Saravanan and E., 2011). In the network level, the security system is critical for protecting both route as well as information forwarding processes. In the absence of accurate security solution, every other malicious node move to play as a widely accessible router, disrupting network connection by incorrectly providing packets, as well as the malicious nodes could provide dull routing updates or fall all packets transferring through them.

Frequency - domain detection is a key method for detecting clone attacks. A clone attack, also known as a node replication attack, is a serious MANET attack (Pietro et al.,2011). An opponent conveys only a tiny set of nodes, reproduces them, but instead assembles an arbitrary set of replicas all throughout system in this attack. It is difficult to tell the difference against a non-compromised node and a CN because a clone has the equal security & code data as the input node. As a outcome, CN could even perform a wide range of another attacks. The detection & protection of cloning attacks in a

MANET is a key issue that could not be easily resolved (Wei and Luo,2011). The current security solutions have the following flaws: highly efficient overheads, the need for central control, unfair assumptions, a lack of smart detecting attacks, and etc. So, by comparing meta-heuristic strategies such as firefly, PSO, genetic algorithm and ACO. For this article, authors propose an ACO method for detecting clones, preventing various attacks, as well as improving network performance.

The simple ACO meta-heuristic exemplifies why this type of technique could execute well in MANET for a number of reasons. The primary reason for this is that the ACO meta-heuristic is predicated on distributed applications as well as works with single ants. This provides a great degree of adaptability to the network's current topology (S.Tsutsui,2008). Another possible explanation is the way of defining the next node, which is focused on the pheromone composition on the existing node and is supplied for every potential connection. The key benefits and drawbacks of ACO are browse in parallel with a population , easily finding effective results, Altered to adjustments like new distances, ACO has a guaranteed convergence (Kavita,2017), The allocation of chances could be changed for every installment, Have a difficult conceptual analysis, Relying patterns of random decisions and high innovative as compared to empirical study.

III. RELATED WORK

There has been a substantial body of studies done in the area of MANET. It includes network delay, link capacity, link consistency, and classifying low mobility nodes. There is research being done on bio - inspired methodologies for routing in communications systems. Even so, an amount of methodologies demonstrate that these ideas could provide better results.

Swapna et al. (2015) MANET could be usually configured in a hostile environment, including a battleground or an actual emergency. MANET routings become more complicated in terms of characteristics like dynamic topology, time-differentiated QoS, limited resources, as well as energy demands. Smart routing protocols, such as the ACO algorithms, demonstrated a promising process for identifying MANET routing protocols. A new QoS optimal solution for MANET has been proposed. The method integrates the ACO motivation with the OLSR) procedure to identify many secure routes to enhance QoS among the source to destination.

Ducatelle et al. (2004) AntHoc Net, a calculation for steering in versatile specially appointed systems in light of thoughts from the Nature-roused Ant Colony Optimization structure. The calculation comprises of both responsive and proactive segments. In a responsive way setup stage, numerous ways are worked between the source and goal of an information session. Information is stochastically spread over the distinctive ways, as per their evaluated quality. Throughout the session, ways are persistently observed and enhanced proactively. Connection disappointments are managed locally. The calculation makes broad utilization of insect like versatile operators which test full ways amongst source and goal hubs in a Monte Carlo form. The consequences of reenactment tests are accounted for in which we have considered the conduct of AntHoc-Net and AODV as a component of hub versatility, territory size and number of hubs. As per the watched comes about, AntHoc Net out performs AODV both as far as end-to-end postpone and conveyance proportion.

Khemchandani and Balkhande, (2014) simulates and analysis the dynamic performance of AntHocNet routing protocol with IEEE 802.11 MAC protocol in random way point model using NS2. Performance of AntHocNet is compared with two reference routing algorithm like Adhoc Online Distance Vector (AODV) and Dynamic Source Routing (DSR) algorithm and the results have been analyzed based on lost packet ratio and normalized routing overhead by varying number of nodes, for different pause time and for different speed.

Sarkar and G. Lol, (2010) investigate the combined effect of node density, packet length and mobility for four routing protocols (OLSR, AODV, DSR, and TORA) on an 802.11 MANET.OPNET-based simulation models has been developed to study the performance of OLSR, AODV, DSR, and TORA for small, medium and large (dense) network scenarios with varying packet length and node mobility. Simulation results obtained show that node density and mobility has a significant impact on underlying routing protocols.

Nancharaiah and Chandra Mohan (2014) suggested a hybrid technique for optimizing MANET routing utilizing ACO and Cuckoo Search. The suggested optimization algorithm uses an ad hoc on-demand vector routing protocol.AODV is optimized based on delays and costs using the proposed algorithm. OPNET was applied to quantify the performance of the proposed optimized routing for AODVs using a network of 100 mobile nodes with a transmission range of 250 m. The nodes are dispersed and move within a 1000m x 1000m area. The target-source pairings are randomly picked from the center

nodes. With a minimum speed of 0 m/sec, a maximum speed of 10 m/sec, &a pause length of 30sec, the random way point model is used for node mobility. Each simulation lasts 900 seconds. The performance of AODV is evaluated using criteria such as average end-to-end delay. When compared to AODV, the suggested algorithm has a shorter end-to-end delay.

Havinalet al. (2016) proposed minimum energy consumption with optimized routing (MECOR), which is a mobile ad hoc network routing protocol. MECOR presents a simple communication strategy based on the mathematical and signaling properties of mobile nodes in MANET to address energy and routing issues in MANET jointly. The MECOR outcome was compared with the conventional routing algorithm as well as recent energy-efficient routing policy studies to find that MECOR can minimize 58.82 per cent of energy in the most challenging MANET mobility scenarios.

Koutet al. (2017) developed a cuckoo search-based reactive routing protocol. The research is divided into two stages. The first phase is the implementation of our approach, and the second is the development of a simulation scenario to test and evaluate our routing protocol, as well as compare it to the AODV, DSDV, and AntHocNet routing protocols. This protocol is applicable to other ad hoc networks, such as vehicular ad hoc networks (VANET) and flying ad hoc networks (FANET).

IV. PROPOSED METHODOLOGY

The key challenge in MANETs is detecting clone attacks. If the clone assault remains unnoticed, the working network will be affected. When a source node has data to deliver to a destination node, it broadcasts forward ants throughout the network to identify a path to the final node. FA will also collect pheromone values from each intermediate node along the way to determine a path to the target node. Backward ants are formed to track the route back to the parent node once the target node has been found. In the network, there are many nodes, but a few of them may be fraudulent nodes. Furthermore, another node in the system may have replicated/cloned the original target node's id. In this case, the fraudulent clone node will send backward agents to the original node. If packets are delivered to the destination's clone, packet loss will occur in the network. When the source node receives backward ants from the clone of the destination node, it will seek help from its immediate one hop neighbors. The source node will send the route request packet again over the path from which backward ants have been received. This time, the destination's id will be scheduled to one of the source node's immediate neighbors in the route request packet. The malicious clone node will again assume the id of the new destination and address back the backward ants to the source node. As a result, the source node will have the same pheromone value for two different destinations, allowing the starting node to recognize the malicious clone node.

V. RESULTS AND DISCUSSIONS

The framework suggested has been implemented using NS2. Network Simulator (Version 2), commonly called NS2, is simply an open-source simulation event-driven instrument which has been shown to be useful to study the dynamic nature of communication systems. NS2 (e.g. routing algorithms, TCP, UDP) is used to replicate assess wired and wireless network functions and protocols. The suggested work estimate a credit-based penalty system on pheromones, residual energy, Euclidean distance, and mobility are the four key elements to consider when optimizing the route toward the source and the target.

- **Pheromone value (PV):** FA agents collect the PV of every intermediate nodes. To optimize the path to the target, the node with the highest pheromone will be found to be the optimum route for packet forwarding.
- **Node residual energy:** The energy left there after a node has received or transmitted packets at any specified period is termed to as the node's residual energy. The MANET mobile nodes are battery-powered and have a limited capacity. Hence, while selecting a pair of intermediate nodes for route formation to a network destination, the battery life of the nodes should be considered. The simple radio energy model was included in this study to forecast the energy required via a node.
- **Euclidean distance:** The Euclidean distance towards the endpoints is the next variable that would determine the optimal route. The distance among the source & the destination must be minimal.
- **Node Mobility**: Node mobility is the unpredictability of a node's movement in a network, which causes network link failure and instability. The optimization route should have fewer mobile nodes in the system.

The system has 60 mobile nodes deployed to begin communication from the source to the destination.

International Journal of IT & Knowledge Management (ISSN: 0973-4414)
Volume 11 • Issue 2 pp. 125-136 Jan 2018 - June 2018 www.csjournals.com

Table 1: Discovered paths from 0 to 59 with PEDM

Path _No	Paths	Pheromone	Energy	Distance	Mobility
0	59 17 14 6 2 0	37.3699	266.815	1031	13
1	59 17 14 6 5 0	16.5447	266.97	1045	17
2	59 17 14 6 10 0	15.6786	267.003	1129	14
3	59 17 14 15 10 0	9.52103	267.02	1108	12
4	59 17 14 16 2 0	10.9181	266.827	1013	11
5	59 17 14 16 5 0	8.51908	266.982	1076	15
6	59 17 14 16 10 0	6.93561	267.015	1067	12

Multiple pathways from sender o to target node 59 have been discovered, as shown in the table 1 above. Among these paths, the path with the highest Pheromone, the highest Residual Energy, the shortest Euclidean Distance, and the fewest mobile nodes will be chosen as the optimal path between sender and receiver. However, according to table 1, route no 0 has the most Pheromone and provides the best route between the sender and the destination node. Path no 3 provides the most residual energy, while path no 4 provides the shortest distance as well as produces less mobile nodes.

But we need a path which gives us optimal route having higher Pheromone, Maximum Residual energy and Minimum distance and minimum mobility nodes. The goal is to establish the hybridized ACO system consisting of a pheromone, the residual node energy and the Euclidean distance and mobility from node to destination. Optimal Path can be obtained by using credit penalty system based on pheromone, the residual node energy and the Euclidean distance and mobility (PEDM). Under this path providing the highest pheromone value, minimum Euclidean distance and maximum RE & various mobile node would rewarded with high points or the reverse will be penalized for routes with minimized pheromone content, fewer remaining energy as well as large routes and providing more mobility nodes.

Table 2: Results of Credit Penalty System Based on PEDM

Path_No	Paths	Results (PEDM)
0	59 17 14 6 2 0	3
1	59 17 14 6 5 0	2.7
2	59 17 14 6 10 0	2.5
3	59 17 14 15 10 0	2.9
4	59 17 14 16 2 0	3.3
5	59 17 14 16 5 0	2.4
6	59 17 14 16 10 0	2.8

The result of the optimized path route, as shown in table 2, is path no 4, which was determined using a Credit Penalty System based on greater Pheromone level, maximum Residual Energy, smallest Euclidean Distance, and less Mobility path. Below demonstrate Simulation Results of ACO/AntHoc Net under Credit Penalty System Based on PEDM.

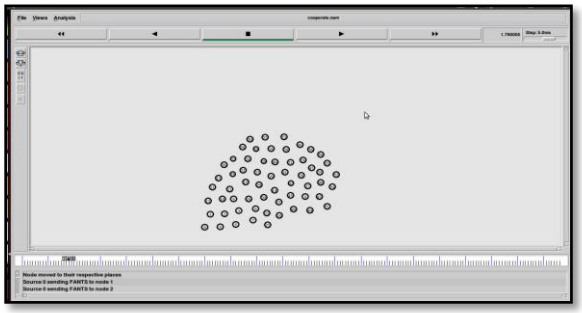

Figure 1: Nodes moving in the network and reached at their respective places

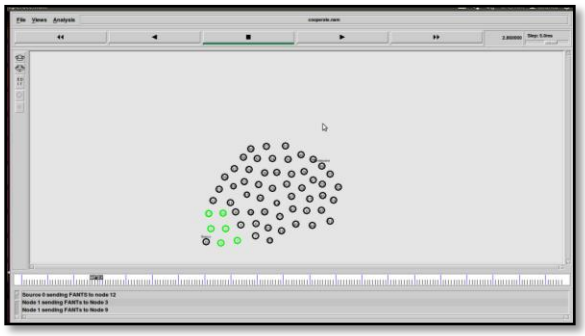

Figure 2: source node o sending FANT to their one hop neighbor nodes

International Journal of IT & Knowledge Management (ISSN: 0973-4414)
Volume 11 • Issue 2 pp. 125-136 Jan 2018 - June 2018 www.csjournals.com

Figure 3: FANT reaches at destination

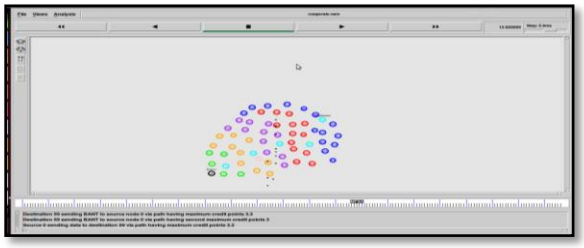

Figure 4: Destination node sending BANT to source node 0 having maximum credit point on the origin of PEDM

The Simulation outcomes for clone attack which are shown in Figure 5 to figure 9.

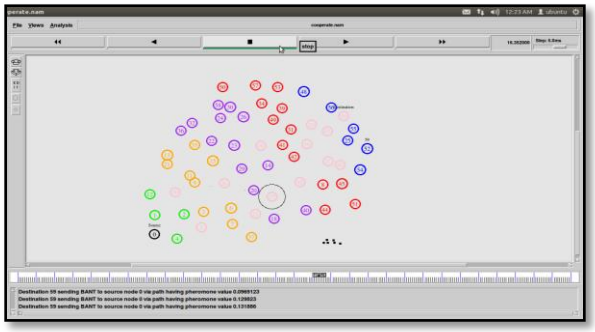

Figure 5: BANT sending return path to source with Pheromone

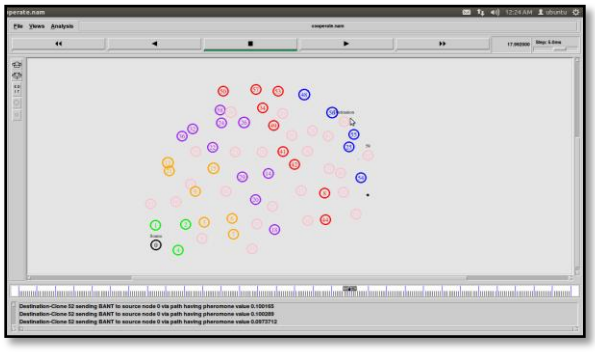

Figure 6: Clone Node sending BANT to source with Pheromone

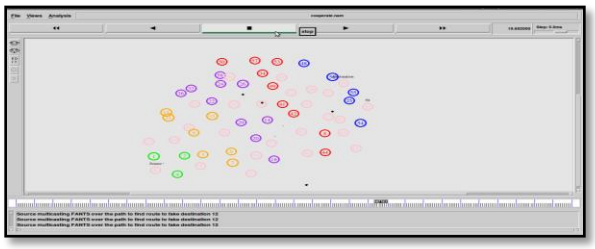

Figure 7: Source Multicasting FANTS across the path to select route to fake destination

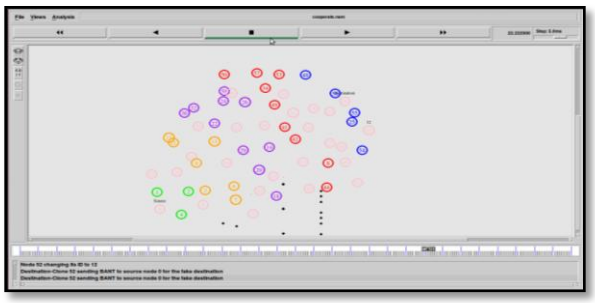

Figure 8: Clone node sending BANT to source node for the fake destination

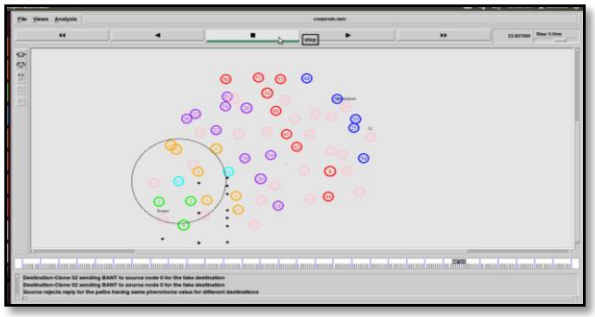

Figure 9: Source refuse reply for the route having similar pheromone value for the new destination

In addition, through implementing a credit penalty-based system on PEDM, different evaluation metrics such as throughput, E2E delay, Jitter, PDR, packet drop, as well as Residual energy have enhanced. When the event is identified with ACO as well as clone detection, the throughput reaches 110 kbps as well as the PDR is 0.44.

VI. CONCLUSION

MANETs utilized as unknown routing mechanisms to cover up node recognitions and/or paths from outside researchers in way to present confidentiality protection. An adversary encapsulates a several nodes, recreates them, & then utilizes an arbitrary set of replicas all through the system in this attack. It is difficult to tell the difference among a non-compromised node as well as a CN because a clone

has the similar safety & code data as the input node. As a result, CN could perform a wide range of other attacks. The identification of cloning attacks is thus a critical issue. The primary idea of this technique is to avoid clone attacks while deploying in MANETs. In this research, the path from source to destination is optimized using modified ACO. The aim of this document was to create a mutated ACO scheme using four variables: pheromone value, residual energy, node mobility, as well as Euclidean distance among nodes. The simulation results of these four variables improved, giving the network a longer lifetime and protecting it from multiple attacks.

REFERENCES

Conti M, Di Pietro R, Mancini LV, A., " Distributed detection of clone attacks in wireless sensor networks", IEEE Trans Depend Security Comp, Vol. 8, pp. 685-698,2011.

Deepak Bansal, Ravinder Singh Sawhney and Ankur Bansal, "Routing Metrics Improvisation in Wireless Mobile Networks Using Ant Colony Optimization" IRAFIT Proceedings published in International Journal of Computer Applications (IJCA),2012.

I. Chlamtac, M. Conti, and J. Liu, "Mobile ad hoc networking: imperatives and challenges", Ad Hoc Networks, No. 1, 2003.

Ishu Varshney, Shahjahan Ali, "Study On Manet: Concepts, Features And Applications" Elk Asia Pacific Journal Of Computer Science And Information System, Vol. 3, No. 2, ISSN(online):2349-9392,2017.

Jing Yang, Mai Xu, Wei Zhao, and Baoguo Xu. , "A Multipath Routing Protocol Based on Clustering and Ant Colony Optimization for Wireless Sensor Networks", Sensors (Basel), Vol. 10, No. 5, pp. 4521–4540, May, 2010.

Jubin Sebastian E, "Performance Comparison of ACO Algorithms for MANETs", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, Issue 1, January 2013.

Kavita Tewani, "Ant colony optimization algorithm: advantages, applications and challenges", computer Modelling & new technologies, Number 21, Issue 2, PP 69-70, April 2017.

Khan, M. S., & Sharma, V., "Ant colony optimization routing in mobile adhoc networks — a survey paper", International Conference on Computing, Communication and Automation (ICCCA), 529-533,2017.

Marinaki, M., and Marnakis, Y., "A Glowworm Swarm Optimization algorithm for the Vehicle Routing Problem with Stochastic Demands", Expert Systems with Applications, Vol. 46, pp. 145-163,2016.

N. Umapathi, N.Ramaraj, "Swarm Intelligence Based Dynamic Source Routing For Improved Quality Of Service", Journal of Theoretical and Applied Information Technology, Vol. 61 , No. 3, March 2014.

Rupérez Cañas, D., Sandoval Orozco, A., García Villalba, L., & Kim, T., "A Family of ACO Routing Protocols for Mobile Ad Hoc Networks", Sensors, Vol. 17, No. 5 ,2017.

Smriti S., Anuj K. Gupta, "Ant Colony Based Dynamic Source Routing", International Journal of Advanced Research in Computer Science and Software Engineering Research Paper, Vol. 3, No.10, October 2013.

S,Tsutsui, "ACO: Ant Colony Optimization", Syst., Control and inform ,Vol.52,No.10 ,pp. 390-398,2008.

Swapna , Priya Jaladi, "Ant Colony Optimization Based Routing to Improve QoS in MANETs", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6, Number 1 , 2015.

Tasbir S., Jaswinder S., "Analysis of Ant Colony Optimization Based Protocols in MANETs", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 8, Aug 2014.