Detection of Black Hole Attack with Ant Colony Optimization

Khushbu

Dr. Bhawesh Kumawat

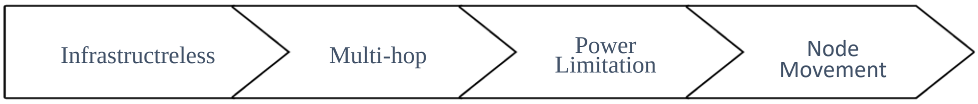
Abstract: A versatile specially appointed organization (MANET) is a decentralized, remote organization wherein hubs impart straightforwardly or through moderate hubs. Exceptional elements like self-setup, decentralized foundation make MANET ideal for use in circumstances of crisis, military tasks, schooling, diversion, sensor organizations and that's only the tip of the iceberg. Notwithstanding the various benefits, MANETs are presented to various assaults influencing their capacity and correspondence with the quick developing geography and the absence of brought together observing. The dark opening assault is perhaps the most broadly archived dynamic assaults that crumble the organization's exhibition and dependability by barring vindictive hubs from every approaching parcel. Various instruments have been advanced as of late to beat the dark opening assault. To keep away from dark opening assault, the current ACO convention has been changed. The arrangement is proposed and mimicked with the Network Simulator form 2 to forestall Black opening assault. As far as parcel conveyance proportion, bundle dropped, normal start to finish delay, yield throughput, remaining energy and steering overhead, the presentation of CUSUM and proposed ACO convention are dissected.

Keywords: Mobile Adhoc Networks, Wireless Network, Black hole Attack, Ant Colony Optimization, Security, CUSUM.

I. INTRODUCTION

Remote organization is progressively developing as remote innovation and the creation of modest cell phones have progressed significantly throughout the last decade. Unconstrained organization sending and transitory help is every now and again required, for example, in military and salvage activities, emergency the executives administrations, virtual study hall meetings, crisis tasks, business organizations, home organizations and area mindfulness administrations, fiasco recuperation activities, and so on In cases like this, sending of "Versatile AD HOC NETWORK" is reasonable choice.

Versatile Ad hoc Networks (MANETs) are networks for a unique, spontaneous assistance that needn't bother with a set up foundation. A MANET (Raza et al. 2016) utilizes radio recurrence (RF) innovation to send and get information through the air medium. These organizations are self-configurable, self-healable and decentralized. In MANETS, hubs are free for example they can meander around and organize. Hubs share a remote channel and the geography of the organization fluctuates progressively due to the portability of versatile hubs. Correspondence normally happens in multi-jump courses, and correspondence is regularly broken, as hubs move self-sufficiently. Notwithstanding different advantages, MANET is helpless against different assaults because of the quick changing geography and absence of incorporated observing. For this situation, certain assurance measures should be set up to guard the MANET against assault (Di Pietro et al., 2014; Sarika et al., 2016). Security is hard for MANETs on account of its provisions, for example, friend and companion engineering, working without a focal facilitator, complex geography, a risky working climate and standard association interruption due to portable hubs, battery life, handling force and heterogeneity. MANET's security needs are equivalent to different organizations for example Honesty, Availability, Confidentiality and Authenticity. Different elements of MANET make it more impervious to different assaults, making it ideal for some genuine applications. These qualities are as per the following:



1.1 SECURITY GOALS IN MANET

The vital goal of safety administrations is to get data and assets from dangers and misconduct. Different security objectives for MANET are as per the following:

• Availability: It guarantees that, regardless of assaults, network administrations are as yet accessible at whatever point they are required.

• Authenticity: It guarantees that there is a legitimate contact between hubs. A malevolent hub doesn't profess to be a dependable hub. The advanced mark plot gives the validation of the message.

• Data Confidentiality: It is the primary security objective of impromptu organizations. It ensures that the trading of messages between two hubs can't be deciphered by another person. The security of information can be cultivated by applying different encryption procedures.

• Integrity: It guarantees that a message sent from sender hub to collector hub was not changed by any vindictive hub during transmission. Advanced mark gives message uprightness.

• Non-Repudiation: It guarantees that the beginning of the message is bona fide. It implies that the sender of the message can't reject that the message has not been gotten. It additionally guarantees that the recipient can't reject that the message has not been gotten. Computerized signature frameworks can be utilized to guarantee that there is no disavowal.

The proposed insect settlement based plan was adequately diverged from the CUSUM (Panos et al. 2017) in this paper. CUSUM gives a grouping number ward recognition strategy for the protection against a dark opening assault. CUSUM requires persistent observing of the addition pace of the arrangement number sooner or later stretches. Anyway this plan is fruitful when the spans are more modest, yet the quantity of parcel drops keeps on expanding as the time stretches increment. This paper presents a novel, settlement based improvement way to deal with guard against a dark opening assault. The pheromone worth of the insects is utilized to distinguish dark opening assaults happening during the information transmission measure.

The early on segment of the paper gives an overall design of the entire paper. This paper is separated into six sections. Segment 2 tends to the different types of assaults in MANET with an accentuation on the Black Hole Attack. Area 3 shows the writing investigation. Area 4 tends to the strategies applied to the dark opening assault utilizing the ACO calculation. Segment 5 tends to the recreation results got after ACO has been executed utilizing network test system (NS2). At long last, Section 6 closures the paper alongside future headings.

II. ASSAULTS IN MANETS

There are two fundamental kinds of organization layer assaults (Rajakumar et al. 2014) in MANET, for example latent and dynamic assaults, which are additionally characterized into a few kinds. In aloof assaults, the aggressor doesn't meddle with the execution of the steering convention, however attempts to check for any valuable data through traffic examination. Detached assaults are truly challenging to identify since the activity of the organization is normal. The motivation behind the gatecrasher is just to gain data that doesn't change or harm the gadget. Encryption of information communicated can go about as a component to forestall a uninvolved assault. Instances of latent assaults are Eavesdropping and Traffic Analysis and Location Disclosure. While a functioning assault can change the information or harm the gadget. A gatecrasher effectively participates in this type of movement and disturbs the every day activity of the organization administrations. These assaults are normally simpler to distinguish than to stay away from, since the assailant can start them in various manners. A few instances of dynamic assaults are displayed in figure 2.1.

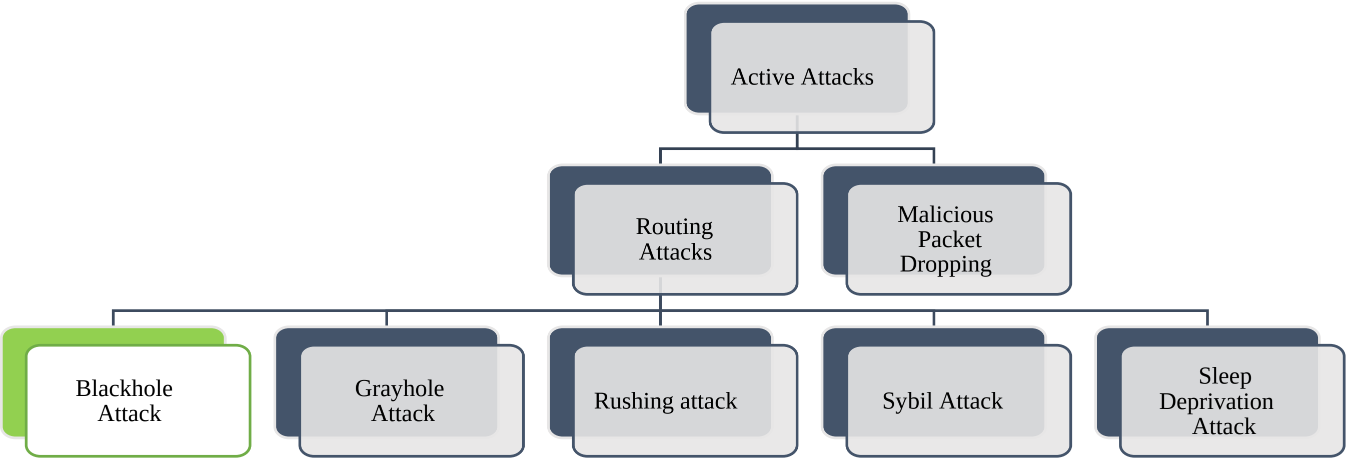


Figure 2.1: Types of Active Attacks

DOI : 10.35291/2454-9150.2022.0006

2.1 BLACK HOLE ATTACK

Dark opening assault in MANETs is a critical security issue that should be handled. A Black Hole assault is a sort of forswearing of administration assault where a pernicious hub sends a bogus answer to a course solicitation and drops a parcel. In this assault, a noxious hub is showcased as having the briefest way to a hub whose bundles it needs to block. Figure 2.2 represents diagrammatically the dark opening assault. As hub P sends a parcel to RREQ, hub Q, M, R gets it. Hub M being a vindictive hub, doesn't confirm the way to hub T with its directing table.

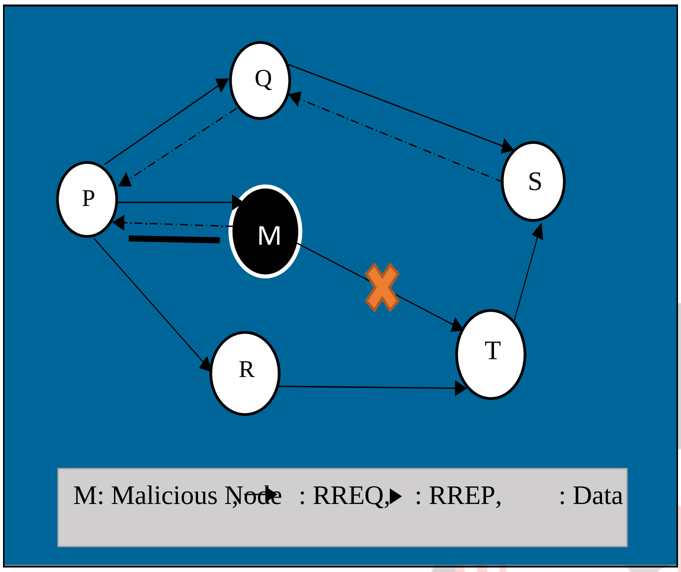


Figure 2.2: Black Hole Attack

There are two properties of the dark opening assault. First the hub utilizes the portable impromptu directing convention, like AODV, to report itself as having a real course to the objective hub, despite the fact that the course is deceptive, fully intent on blocking bundles. Second, the aggressor devours bundles that have been blocked with no sending. The aggressor, nonetheless, runs the danger that the encompassing/adjoining hubs will follow and uncover the continuous assaults. There is a more unpretentious kind of these assaults when the assailant advances bundles specifically. An assailant stifles or changes bundles beginning from certain hubs while leaving the information from different hubs unaltered, which decreases the assumption of their bad behavior.

III. WRITING REVIEW

One of the security assaults that happen in remote portable specially appointed organizations is the dark opening assault. Interlopers utilize the secondary passage to execute their malevolent activities on the grounds that the course of course revelation is fundamental and unavoidable. Numerous analysts have utilized different discovery methods to propose various types of identification plans.

Nancharaiah and Chandra Mohan (2014) presented the use of ACO with CS (Cuckoo Search) to the advancement of directing issues in MANETs. ACO directing strategies are effortlessly custom fitted to handle the very difficult conditions of MANETs. It is shown that the proposed mixture calculation (ACO with CS) performs better as far as throughput, normal start to finish delay, absolute reserved reactions sent and course time securing contrasted with existing calculations.

Abdelshafy et al. (2016) presented the possibility of self-convention trustiness (SPT) in which the ID of a vindictive gatecrasher is accomplished by consenting to normal convention conduct and drawing the malignant hub to give implied evidence of its noxious conduct. Another Black hole Resisting Mechanism (BRM) is executed that can be coordinated into any MANET receptive directing convention. The system didn't utilize cryptographic procedures that save force and figuring assets. Moreover the interaction didn't need any extra bundles and accordingly doesn't cause any extra overheads. The reproduction results showed that BRM-AODV conveys a gigantic improvement in network effectiveness in all organization measurements through both AODV and SAODV.

Yasin and Abu Zant (2018) have presented a savvy dark opening recognition and detachment method that ought to be viewed as while building and further developing any dark opening battle conventions or strategies. The proposed TBBT joins the two clocks and teasing strategies with the end goal of upgrading dark opening recognition capacities while keeping up with throughput, start to finish postponement, and bundle conveyance proportion.

Hamamreh (2018) proposed Improved RID-AODV to distinguish and moderate the impacts of various dark opening assaults in MANETs pointed toward expanding throughput and PDR while lessening the normal start to finish deferral and overhead. It is an improved and refreshed variation of the instrument recently proposed, RID-AODV. In light of the reproduction execution, Improved RID-AODV offers a higher throughput and parcel transmission proportion than its past emphasis. Dynamic boycotts additionally effectsly affect the decrease of the overhead proportion and the start to finish delay.

DOI : 10.35291/2454-9150.2022.0006

Shivamallaih and Karibasappa (2018) proposed ACO-DRSA-BD calculation to exactly recognize the BH Node (BHN) to track down the right answer for ACO information transmission and DRSA safe climate. ACO permits to take another course in case there is a malevolent hub in the organization. Information is encoded utilizing the Dual Rivest-Shamir-Adleman (DRSA) strategy and Black Hole Detection (BD) is utilized to find malignant hubs on the organization. Out of the reenactment results it was presumed that the ACO-DRSABD approach accomplished the best directing and better throughput, overhead steering and energy contrasted with the AODV calculations by conveying various hubs. Accordingly, the throughput in ACO-DRSA-BD is 10% higher than the AODV cycle. Overhead directing in ACODRSA-BD is 22% lower than the AODV cycle. Energy utilization diminished by 5% contrasted with the AODV cycle.

Junnarkar et al. (2018) introduced a QoS effective ACO-based directing calculation that utilizes hub area data to determine MANET portability issues. This strategy called the QMAA directing convention, is a course choice framework created utilizing the FANT and BANT rules for course determination. With a security calculation, the QoS-cognizant convention is proposed named as Secure-QMAA (SQMAA). SQMAA accomplished safe correspondences while ensured QoS productivity against existing steering conventions. The recreation results show that within the sight of noxious aggressors, SQMAA execution is effective contrasted with QMAA and the cutting edge directing convention.

El-Semary and Diab (2019) presented a steady MANET directing convention called BP-AODV to determine security breaks identified with the Secure AODV (SAODV) convention alongside the first AODV convention. Likewise, the BPAODV is fit for safeguarding against an agreeable blackhole assault started during the steering system and secures against a blackhole assault that can happen during the sending system. BP-AODV is worked by growing the usefulness of the AODV convention alongside the utilization of tumultuous guide highlights.

Naveena et al. (2020) proposed a trust-based directing plan to find a gatecrasher hub on a versatile organization. The proposed approach is grouped in the Data Retrieval (DR) table, to distinguish and keep up with every hub information move measure in the steering climate and course creation stage, and to foresee the protected way to the exchange of the information parcel to the objective hub. The blackhole assault is noticed, which diminishes the drop proportion of the parcel. Khan et al. (2020) presented Ant Colony Optimization Technique and Repetitive Route Configuration with Reactive Routing Protocol to hinder dark opening Attack in versatile specially appointed organizations.

Ourouss et al. (2020) proposed ACO DSR dependent on the standing consolidated the beta rating framework with ACO metaeuristic to genuinely survey the trust of the hub as far as the exchange of bundles in the interest of its participation. The model proposed fortifies the standard Dynamic Source Routing (DSR) convention by disengaging pernicious hubs from information parcel investment. Disregarding the presence of some dark opening, the RACODSR uncovers that the standing based ACO DSR (RACODSR) surpasses DSR standard for the bundle misfortune proportion with an increment of 0.22 percent, by an increment of 0.4 percent in the DSR parcel misfortune proportion with an abatement of 22.76 percent in the end-toend delay.

IV. METHODOLOGY

Ant Colony improvement can assist with identifying the dark opening assault in the proposed project. As the source hub starts the most common way of discovering the way to the objective hub, each halfway hub can act as a noxious hub and can flood its whole neighborhood with countless course demand parcels. In the event that the solicitation arrives at its objective, the objective reacts back to the source hub by means of different potential ways. The source hub chooses another course dependent on the most noteworthy worth of the course answer parcel arrangement number. Any middle hub arranged as a dark opening aggressor pushes the grouping number to an exceptionally high worth. So the source hub picks the course that has a malevolent hub. The malevolent hub drops it when the information is gotten. In this way the dark opening assault happens during the reaction cycle of the way.

When the malevolent flooding hub gets distinguished in the organization as noxious, the way discovering stage will keep as indicated by its ordinary conduct. In the event that the forward insects demand hits the objective hub, some pheromones are likewise saved at the objective hub.

Assume 'Pde' be the measure of pheromone stored over it. Say dissipation of pheromone is E. While objective hub sends back Route answer or ANTBR towards the source hub, a specific measure of pheromone will begin being dissipated. Assume there are 'η' number of ways set up at the objective hub over which the objective has sent ANTBR towards the source hub. Each course is comprised of 'Ni' number of middle of the road hubs.

The time taken by the course answer or by every one of the insects to arrive at the source hub is as per the following:

Back Time = (1)

Where t s(p) is when group is sent over that way by downlink center point and t r(p-1) is when package is gotten by the uplink center in the manner including Ni number of center points.

DOI : 10.35291/2454-9150.2022.0006

A restricted amount of pheromone is disappeared from the target center during this time.

Pheromone Evaporated = pde X E X $\sum Nip=-11\ ts\ (p) - tr\ (p-1)$ (2)

Remaining Pheromone = Pde X pde X E X $\sum Nip=-11\ ts\ (p) - tr\ (p-1)$ (3)

The best course to arrive at the objective hub will be picked at the source hub. At the point when you begin sending an information parcel over the picked way to the objective hub, the time the bundle takes to arrive at the objective is:

Send Time = $\sum Np=-11\ t(p) - tr(p-1)$ (4)

The objective hub should begin tolerating information bundles all at once equivalent to the measure of Back Time and Send Time.

Stand by Time = (5)

Presently the amount of pheromone left at the objective will be:

Pheromone left = Pde - pde X E X $\sum Nip=-11\ ts\ (p) - tr\ (p-1) - \sum Nip=-11\ ts\ (p) - tr\ (p-1)$ (6)

This measure of pheromone can be seen as a base measure of pheromone that can be left at the objective hub before it starts to acknowledge information parcels, in which case the pheromone will begin to be kept once more. In the event that the objective hub sees that less pheromones are left and no information parcels have been acquired, it will send NACK over the ways to the source hub. In the event that the source hub sent parcels over the dark opening hub way, the sending of information will be ended. To confirm what hub has not forward any parcels, the objective hub would send "Question bundle" to the source hub through the ways it sent course answers. In the event that hubs have not gotten bundles from their uplink hub, they will report a similar objective. The uplink hub is marked as malevolent and the objective hub tells the source hub also. Presently the source hub will choose the course without pernicious hub to continue information transmission.

V. SIMULATION RESULTS

In open source network test system 2.35, the two plans, CUSUM and ACO-based discovery plot were presented. In the 1200*1200 sq. meter the organization has been worked with seventy hubs moving alone as per the Random Way Mobility Model. Meters. Meters. Table 4.1 characterizes all recreation boundaries.

Table 4.1: Simulation Parameters Used

Parameter	Value
Channel	Wireless
Mac	802.11
Radio Propagation Model	Two Ray Ground
Antenna	Omni Directional
Number of nodes	70
Bandwidth	1Mb
Initial energy	60 Joules
Area	1200*1200 sq. meters
Mobility model	Random Way Point
Traffic Type	CBR
Queue	Drop Tail
Mobility	0-5 m/s
Energy Model	First Order Radio Dissipation Energy Model

5.1 Execution Metrics

Six boundaries were utilized for examination of the organization execution:

Throughput: This is the amount of information got per unit of time at the objective hub. Not really set in stone under the single source-objective pair situation in the organization at the objective hub.

Throughput = (Number of bundles got * Size of every parcel)/Time

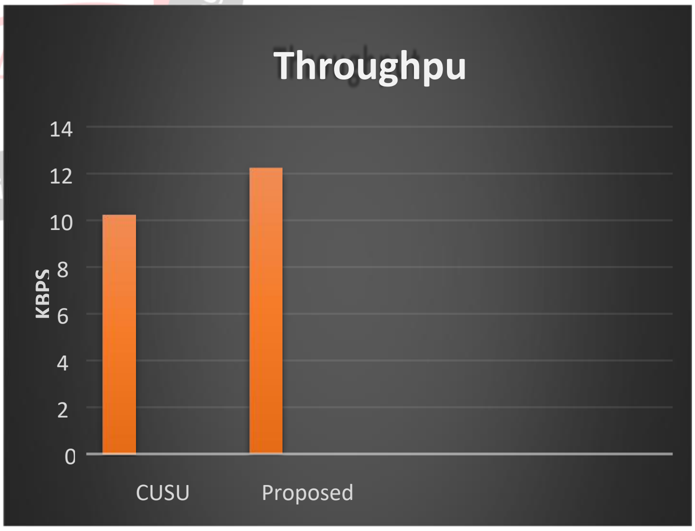


Figure 4.1: Throughput

According to the strides for the qualities got for the bundle conveyance proportion, the throughput likewise showed higher qualities for the proposed ACO-based plan. Huge measure of blockage made in the organization under CUSUM plot lead to utilization of transfer speed of the connections. This was justification corrupted throughput esteem. This likewise requires more transmission capacity

DOI : 10.35291/2454-9150.2022.0006

utilization. The incentive for the throughput was found at 122 Kbps for ACO based plan and 102 Kbps for CUSUM.

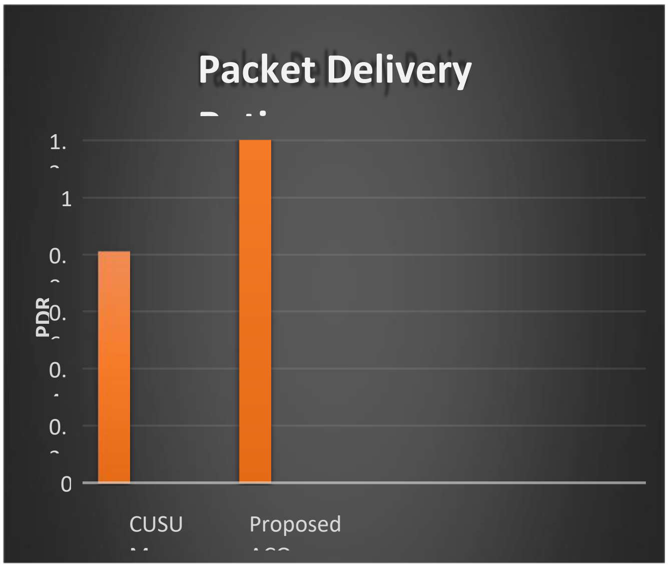


Figure 4.2: Packet Delivery Ratio

Packet Delivery Ratio: Bundle Delivery Ratio: This is a proportion between the measure of information parcels got over the organization and the quantity of parcels sent over the organization.

PDR = Number of information bundles got/Number of information parcels sent

The level of bundles followed through on an organization is portrayed in Figure 4.2. The two assaults can be recognized in contrasted with CUSUM in the proposed ACO based plan (that exclusively identifies dark opening assault). In CUSUM, just the dark opening hub during transmission can be utilized to drop the parcels. This decides fixed time spans to confirm the rate at which arrangement numbers will be expanded in the organization. As the time span expands, the five dark opening hub is bound to get information from the source hub and in this manner drop it. At the point when the dark opening assault is happening, the ACObased conspire is sitting tight for some time until the objective hub stops sending source hub bundles when the pheromone has dissipated over it. This raises the bundle conveyance proportion of the proposed location plot dependent on the ACO.

Number of bundle drops: This shows the number of parcels is falling on the organization.

Packet Drops = Number of parcels sent – Number of parcels got

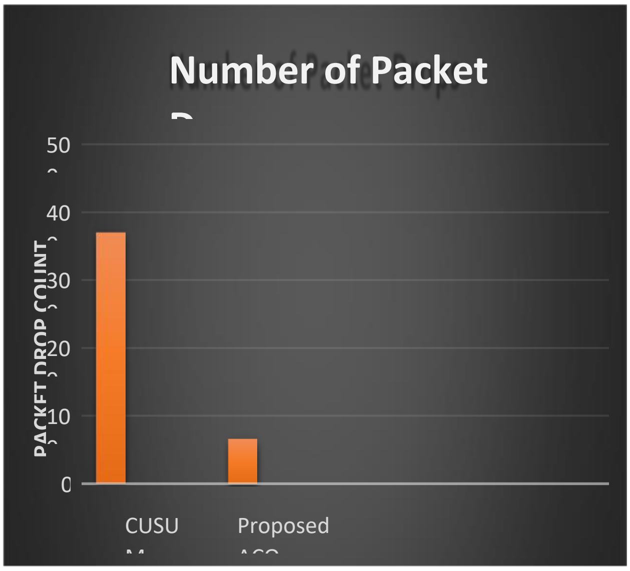


Figure 4.3: Number of Packet Drops

Chart 4.3 breaks down the effect of assaults on the organization as far as the real number of bundles dropped by the vindictive hub. Since CUSUM has lower time stretches to figure the pace of progress of grouping number, the quantity of bundle drops is lower. Then again, the proposed conspire was observed to be more powerful than both of the two plans as far as number of bundle drops in the organization.

Directing overhead: This is characterized as an extent of the quantity of control bundles communicated in the organization and the quantity of got information parcels.

Overhead = Number of control bundles sent/Number of information parcels got

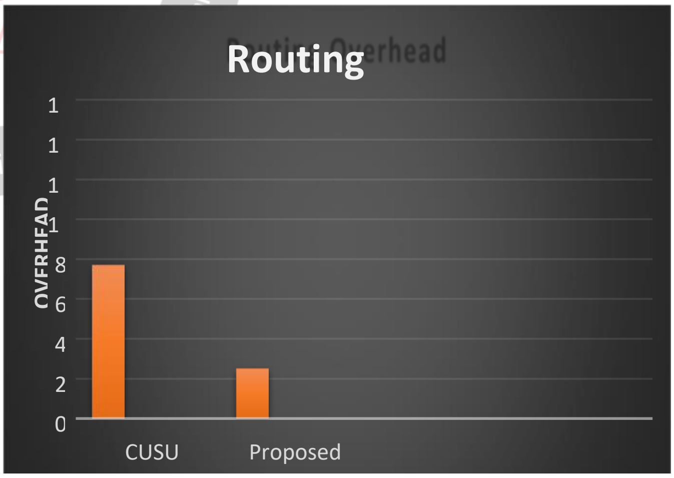


Figure 4.4: Routing Overhead

The directing overhead addresses the measure of control parcels needed to be sent in the organization for conveyance of information at the objective hub. In the event of CUSUM, preparing of the organization to distinguish pace of progress of grouping numbers prompts more control bundles sent in the organization. The ACO based plan permits the assault to occur for tiny measure of time,

DOI : 10.35291/2454-9150.2022.0006

this prompts least benefit of steering overhead among every one of the plans.

Remaining energy: This mirrors the amount of energy left over in the organization..

Remaining energy = Initial Energy – Energy devoured.

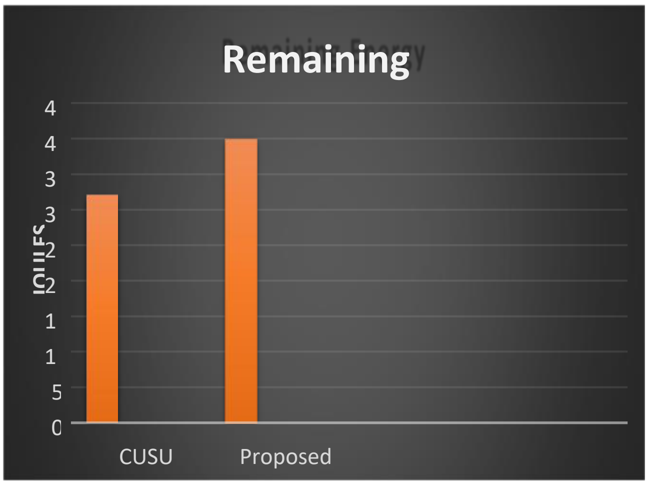


Figure 4.5: Remaining Energy

Figure 4.5 provides a good understanding of how much energy the network uses to identify malicious nodes. All nodes earned initial energy of 60 Joules in the network. The CUSUM scheme must have patterns for the rate of change of sequence number under normal conditions. The network is then evaluated under the presence of a malicious black hole node in the network. This scheme therefore requires an extra amount of energy to train the network. ACO dependent scheme includes a single simulation run to detect malicious nodes in the network. The proposed ACO scheme consumes 39.96 Joules of energy, while CUSUM consumes 32.08 Joules of energy.

Average end-to-end delay: This is average of difference between the time at which packets are received and the time at which packets are sent in the network.

Average E2E delay = (Packets Receiving time – Packets sent time) / number of packets.

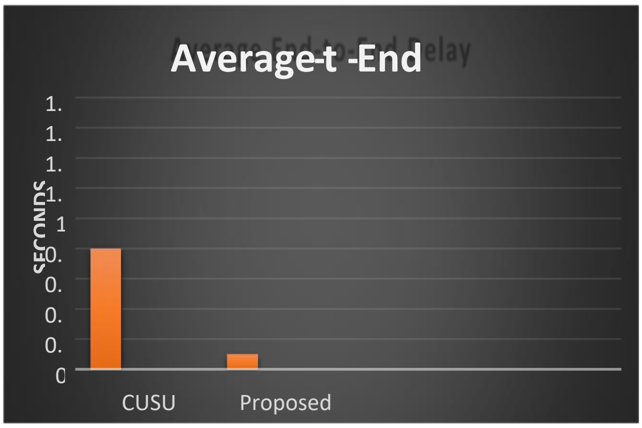


Figure 4.6: Average End-to-End Delay

This parameter has been determined for each packet sent to the network under these two schemes. It was noted that the delay was the least for the proposed ACO-based scheme equivalent to the CUSUM. The only reason for higher value for the CUSUM scheme was due to the large number of packets sent to the network that are needed for the detection process (training of the network through the CUSUM broadcast process).

VI. Conclusion and Future Work

The work describes the defense of the mobile ad hoc network against the black hole attack occurring during the data transmission phase, by using ant colony optimization algorithm. The work has been extensively compared with black hole attack defense mechanism named CUSUM. The CUSUM scheme requires the training of the network for more than one simulation runs to notice the rate of change of sequence numbers. CUSUM needs to operate in the attacker-free environment to train the network. This leads to consumption of network resources. The ACO based scheme on the other hand, requires only pheromone levels calculation and adjusting the pheromone levels to detect the malicious black hole node in the network. It is independent of rate of change of sequence number and in addition it does not requires training the network or monitoring the network for a significant amount of time. Thus, this scheme saves network resources and improves performance of the network.

In future, this scheme can be analyzed for varying number of attackers and under different mobility scenarios. This work defends the malicious nodes by setting the pheromone levels to a particular threshold values. This involves the deposition as well as evaporation rate of the pheromones. Furthermore, in future, the work can be analyzed at different evaporation and deposition rates of the pheromone levels.

References

[1] Abdelshafy, M. A., & King, P. J. B. (2016). Resisting blackhole attacks on MANETs. 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC).

[2] Di Pietro, R., Guarino, S., Verde, N. V., & Domingo-Ferrer, J. (2014). Security in wireless ad-hoc networks – A survey. Computer Communications, 51, 1–20.

[3] El-Semary, A. M., & Diab, H. (2019). BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs based on Chaotic Map. IEEE Access, 1-17.

[4] Hamamreh, R. A. (2018). Protocol for Multiple Black Hole Attack Avoidance in Mobile Ad Hoc Networks. Recent Advances in Cryptography and Network Security.

[5] Junnarkar, A. A., Singh, Y. P., & Deshpande, V. S. (2018). SQMAA: Security, QoS and Mobility Aware

DOI : 10.35291/2454-9150.2022.0006

ACO Based Opportunistic Routing Protocol for MANET. 2018 4th International Conference for Convergence in Technology (I2CT), 1-6.

[6] Khan, D. M., Aslam, T., Akhtar, N., Qadri, S., Rabbani, I. M., & Aslam, M. (2020). Black Hole Attack Prevention in Mobile Ad-hoc Network (MANET) Using Ant Colony Optimization Technique. Informacines Technologijos IR Valdymas, 49(3).

[7] Nancharaiah, B., & Chandra Mohan, B. (2014). Hybrid optimization using Ant Colony Optimization and Cuckoo Search in MANET routing. 2014 International Conference on Communication and Signal Processing, 1729-1734.

[8] Naveena, S., Senthilkumar, C., & Manikandan, T. (2020). Analysis and Countermeasures of BlackHole Attack in MANET by Employing Trust-Based Routing. 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS).

[9] Ourouss, K., Naja, N., & Jamali, A. (2020). Defending Against Smart Grayhole Attack within

[10] MANETs: A Reputation-Based Ant Colony Optimization Approach for Secure Route Discovery in DSR Protocol. Wireless Personal Communications, 33(18).

[11] Panos, C., Ntantogian, C., Malliaros, S., & Xenakis, C. (2017). Analyzing, quantifying, and detecting the blackhole attack in infrastructure-less networks. Computer Networks, 113, 94– 110.

[12] Rajakumar, P., Prasanna, V.T. & Pitchaikkannu, A., 2014. Security attacks and detection schemes in MANET. 2014 International Conference on Electronics and Communication Systems, ICECS 2014.

[13] Raza, N., Aftab M. U., & Akbar, M. Q. (2016). Mobile Ad-Hoc Networks Applications and Its Challenges. Communications and Network, 8(8), 131–136.

[14] Sarika, S., Pravin, A., Vijayakumar, A., & Selvamani, K. (2016). Security Issues in Mobile Ad Hoc Networks. Procedia Computer Science, 92, 329–335.

[15] Shivamallaih, S. M. & Karibasappa, K. (2018). An Efficient Detection of BH Attack with Secured Routing Using ACO and DualRSA in MANETs. International Journal of Intelligent Engineering & Systems. 11(2), 246-255.

[16] Siddiqua, A., Sridevi, K., & Mohammed, A. A. K. (2015). Preventing black hole attacks in MANETs using secure knowledge algorithm. 2015 International Conference on Signal Processing and Communication Engineering Systems.

[17] Yasin, A., & Abu Zant, M. (2018). Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. Wireless Communications and Mobile Computing, 2018, 1– 10.