January-February 2020
ISSN: 0193-4120 Page No. 8276 - 8281

Comparative Analysis of LEEAR, AFDP and ARPASC Routing Protocols in MANETs

[1]A. Naveena, Assistant Professor, ETM, [2]Dr. K. Rama Linga Reddy,
Professor, HOD, ETM dept.GNarayanamma Institute of Technology and Science for Women

Article Info
Volume 82
Page Number: 8276 - 8281
Publication Issue:
January-February 2020

Article History
Article Received: 18 May 2019
Revised: 14 July 2019
Accepted: 22 December 2019
Publication: 07 February 2020

Abstract:
The recent development made in mobile technologies has demanding increase of secured networks in real-time applications. Security is more significant in Mobile Adhoc Network than in wired environment. When two or more different attackers collaborate together to interrupt the network performance it results in collaborative attacks. Due to lack of resources and centralized authority, these collaborative attacks have to be handled effectively. Prior security protocols may not be appropriate or may compromise the Network performance. In this paper three proposed techniques: hybrid security protocol for detecting malicious nodes, distributed anonymity fault diagnosis protocol and Adaptive risk prediction protocol are compared. The performance metrics are evaluated in terms of Packet Delivery Ratio (PDR), End-to-End delay, Throughput, Energy Consumption using NS2..

Keywords:*Anonymity, blackhole, greyhole, risk evidence, trapdoor, zero knowledge proof.*

I. INTRODUCTION

The technological advancement made in wireless technologies has greater impact among the wireless users. In general, MANET composes of dynamic, self- arranged and self-deployed group of nodes where each node acts as a router. This environment will not rely on any centralized architecture due to their adhoc nature. Mobility is a significant parameter in MANET environment. Most of the network protocols aim to be attack-resilient rather than discarding the attack sources. Even though, the resiliency model detects the threats, the time consumed for detecting new type of attacks is still in vain. The main source of attacks is to compromise the nodes by disrupting the network services. The effect is even worst when these attackers collude with each other and collaboratively attack the network [8] [9] [10].

Collaborative attack is one of the most vulnerable threats in routing process of mobile adhoc networks. It belongs to a class of synchronized attacks where more attackers are involved to interrupt the routing services of the network. When two or more intruder involves synchronizing the actions to interrupt the target networks, it constitutes as collaborative attack. There are different routing attacks like wormhole attacks, blackhole attacks and greyhole attacks. These attacks collaborate with each other and try to disrupt
the network services. Privacy preservation is an important concept to achieve better security system [2].The acquisition of data from different sources of network exposes different
security challenges. Even though, lot of security techniques supports the data protection process, integrity of the data is not achieved.
Anonymization [1] is one of the efficient techniques used for enhancing the security and network performance of the systems. Since MANET environment is open in nature, data may get lost or tampered by threatening the routing protocols. This

January-February 2020
ISSN: 0193-4120 Page No. 8276 - 8281

scenario is resolved by anonymous routing protocols. The term anonymity refers to concealment of identity of the source, destination and the selected path. With the help of anonymization protocols, secured communications is possible by hiding node identities and thus preventing the attacks. It applies to banking, military etc. The defending of collaborative attacks often utilizes anonymization techniques, as a solution to the data protection issue. Data privacy is maintained by using anonymization techniques [3] [4].

II.PROPOSED TECHNIQUES

2.1 Lightweight Energy Efficient Anonymous Routing Protocol (LEEAR):

The wireless communication medium is open in nature and the possibility of advertising the false information to the network is higher that degrades the performance of the system [6].. The protocol consists of following phases [17] :

- Implementation of trapdoor protocol using zero-knowledge proof [5].
- Anonymous route discovery phase [7].
- Anonymous route reply phase.
- Anonymous data transfer phase

Anonymous route discovery phase:

In this phase trapdoor protocol is used along with the bloom filter. Since trapdoor is used only true destination can open the trapdoor.Bloom filter ensure efficient routing.

Anonymous route reply phase:

In anonymous route discovery phase, when the destination node has received the RREQ message:

- If the destination node D has already shared a session key with its ancestor node, it constructs the RREP message as following: $<NRREP, N_{X,X+1}, E_{K_{X,X+1}}(Seqnum, K_f^{'})>$ where $K_f^{'}$ is the commitment value of K_f.
- If there is no session key between them, the constructed RREP message is :

$< ARREP, E_{APX_X}(K_{X,X+1}, N_{X,X+1}) E_{K_{X,X+1}}(Seqnum, K_f^{'})$Checks if $E_{K_f^{'}}$(seqnum) = E_{K_f} (seqnum), If true destination is valid node or else invalid node.

6.1.3 Anonymous data transfer phase:

In anonymous data transfer path, after the establishment of the anonymous path, data transfer takes place providing security to the data by using pseudonym (N) and encrypting the data with shared keys.

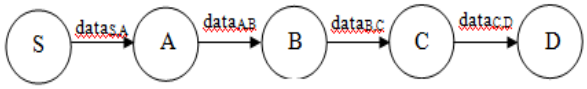

Fig.2.1 Anonymous data transfer phase

$$\text{data}_{S,A} =< N_{S,A}, E_{K_{S,A}}\left(N'_{S,A}, E_{K_{S,D}}(\text{data})\right) >$$
$$\text{data}_{A,B} =< N_{A,B}, E_{K_{A,B}}\left(N'_{A,B}, E_{K_{S,D}}(\text{data})\right) >$$

2.2. Anonymity Fault Diagnosis Protocol for MANET

Anonymous routing protocol efficiency can be enhanced by incorporating fault diagnosis [15]. In the fault diagnosis model, the node trust level is diagnosed based on the node anonymity fault probability function $TA(q)$. Based on the characteristic matrix, the maximum probability of interaction is measured as $P(\beta_i) = log_2 N_i(x_i, y_i)$, where (x_i, y_i) are the node N coordinates and the mobility probability is measured as $P(\alpha_i) = \sum_{i=1}^{n} s_i\,(x_i, y_i) * t$, where s_i is the speed of the node and t is the time.

$$TA(q) = \{P(\beta_i), P(\alpha_i)\} \qquad (1)$$

Based on the characteristic matrix, an anonymity fault diagnosis protocol organizes the diagnosis packet at source node or transmitter node by computing the anonymity fault diagnosis function.

$$F_{ij}(t) = P(\alpha_{ij}) P(\beta_{ij}) \qquad (2)$$

January-February 2020
ISSN: 0193-4120 Page No. 8276 - 8281

Anonymity RREQ Fault Diagnosis Format

Fault diagnosis route discovery initiate a route discovery process by creating fault diagnosis route packet [12]. Upon receiving a packet from source node by the forwarder node or neighbor node, the hop count mhc is decreased by 1 and flag type compute the fault diagnosis function to validate the node. If the fault diagnosis function is less than the threshold rate value, then the ftype change the mode as True, if not the ftype mode will be a False.

Anonymous route discovery process:

Let n be the number of nodes in a network and b be the number of bits to denote a node in the routing vector. To inspect this process, the anonymity route discovery process initializes bit vector and route vector. The route vector represents set of bits for corresponding nodes. The following steps determine the route anonymized route discovery process.

Step 1: Initialize routing vector $n * b \leftarrow 0 \; \forall \; n$.

Step 2: Identify the optimal node with high probability functional weightage calculated based on speed and energy of the nodes and set the bit vector for visited node as 1 and unvisited node as 0.

Step 3: Set next routing vector with $b - bits$ based on visited and unvisited factor function $R(n)$as :

$$R(n) = (m * \mathrm{b}) + 1)^{th}$$

Step 4: Repeat step-3 to identify the destination and set routing vector.

Secure Data Forwarding

When the secrecy shortcoming end model approves the hubs and finds the direction, the proposed convention creates a fantastic direction [13]. This thrilling pen name is applied to talk to an data sending manner. The source typifies the facts bundles and disseminates the parcels on over the determined course and updates the course pen call into the direction disclosure table. Each forwarder hub have to investigate the route revelation table to approve the hub verification. In the occasion that it is not coordinated it disposes of the package deal.

2.3 Adaptive Risk Prediction and Anonymous Secured Communication in MANET

ARPASC is proposed to predict the risks and identify the attacks before processing anonymous communication [15].

Risk Estimation:

$$Risk\ Estimation\ probability = f(a, d, m, ct) \quad (3)$$

Where a= Angle, d = Distance, m = Mobility, ct = Compromise Time.

Angle probability:

$$p(a_k) = 0.5X\left(1 - \frac{\theta_k}{(\sum_{k=1}^{3} \theta_k)}\right) \quad (4)$$

Distance probability:

$$dist_{(i_0,j_0)(i_k,j_k)} = \sqrt{(j_k - j_0)^2 + (i_k - i_0)^2 + (j_k - j_0) \times (i_k - i_0)} \quad (5)$$

$$p(d_k) = \frac{dist_k}{(\sum_{k=1}^{3} dist_k)} \text{where} dist_k = \log_{10} dist_{(i_0,j_0)(i_k,j_k)}, \quad (6)$$

Compromise time probability:

$$p(ct_k) = \frac{1-ct_k}{(\sum_{k=1}^{3}(1-ct_k))} \text{where} ct_k = \sum_{i=1}^{n} \frac{1}{t_i vs_i}$$, where i= {1 to n}, n is number of vulnerabilities. (7)

Consider t = 1 unit., vs_i is the vulnerability severity.

Mobility probability:

$$p(m_k) = \left(1 - \frac{m_k}{(\sum_{1}^{3} m_k)}\right), \text{where} m_k = rand(v),$$ where v isvelocity which represent the node mobility speed. (8)

Path Vulnerability Estimation

Algorithm[16]:

1) Initialize set of states $s = \{s_1, s_2, \ldots, s_i\}$ where $s_i = \{p(a_k), p(d_k), p(M_k), p(ct_k)\}$ (9)

January-February 2020
ISSN: 0193-4120 Page No. 8276 - 8281

2) Generate random observation states $\{v_1, v_2, \dots, v_M\}$
3) Calculate risk estimation transition probability

5.1 transition probabilities $REP_{ij} = P(s_i|s_j)$

$P(\{p(a_k), p(d_k), p(m_k), p(ct_k)\}) =$
$P\left(\left(\frac{p(a_k)}{p(d_k)}\right) P\left(\frac{p(d_k)}{p(m_k)}\right) P\left(\frac{p(ct_k)}{p(d_k)}\right)\right)$ (10)

5.2 observation probabilities

$B = P(v_m \mid s_i)$ (11)

5.3 initial probabilities

$\pi = (\pi_i), \ \pi_i = P(s_{ik})$ (12)

4) Find the probability of minimum and maximum number of hops using the transition matrix.

5) The overall transition vulnerability estimation probability is

$P(VE) = (H_{min}, H_{max}, REP_{ij}, B, \pi)$ (13)

Risk Evidence Collection:

The risk of each path and risk of each adjacent node is obtained by the risk evidence collection based on entropy and information gain calculations. Estimate entropy of each path to determine uncertainty by considering risk estimation matrix data[14].

$H(S) = \sum_{c \in C} -p(c) \log_2 p(c)$ (14)

where S represents set of path states.

C represents set of classes $\{H_{min}, H_{max}, REP_{ij}, B, \pi\}$.

$p(c)$represents the proportions of number of elements in a class C.

Entropy value set will be assigned to information gain for determining the path efficiency.

$IG(A, S) = H(S) - \sum_{t \in val(A)} p(t) H(t)$ (15)

$H(S)$entropy of set S.

A : Attribute set

The risk evidence considers two different evidences types $RE1, RE2$, where $RE1$ is possibility of attack occurrence in a chosen path in between source and destination pair. The risk evidence probability is represented as

$P(RE1) = f(IG(S))$ (16)

where the $f(IG(S))$ is a probability attack function which is a representation of information gain attribute rate.

$\min(IG) < P(RE1) \leq \max(IG)$will be considered.

$P(RE2)$: proves an evidence of path alter by malicious node, where the path alter function $f(P)$considers the minimum and maximum hop values $\{H_{min}, H_{max}\}$ and different distance rates.

$P(RE2) = f(P)$ (17)

Attack = P(RE1) $\oplus$ P(RE2) (18)

III. SIMULATION RESULTS

Comparative analysis is done for all the three proposed LEEAR, AFDP and ARPASC protocols in this paper. The results [17] demonstrate that the ARPASC protocol is efficient than LEEAR and AFDP protocols with respect to PDR, Throughput, Energy consumption and E2E Delay.. PDR of ARPASC is 6.5% more than LEEAR and 5.5% more than AFDP.Throughput of ARPASC is 10% more than LEEAR and 7% more than AFDP.Energy Consumption of ARPASC is 14.9% less than LEEAR and 10% less than AFDP. E2E Delay of ARPASC is 6.5% less than LEEAR and 5% less than AFDP

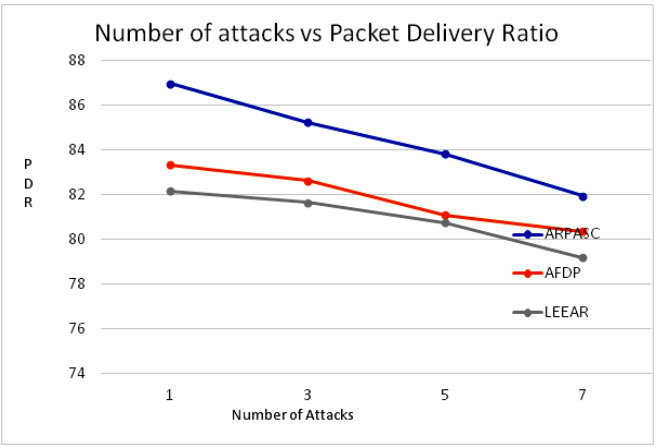

Fig.2.2 PDR Vs Attacks

January-February 2020
ISSN: 0193-4120 Page No. 8276 - 8281

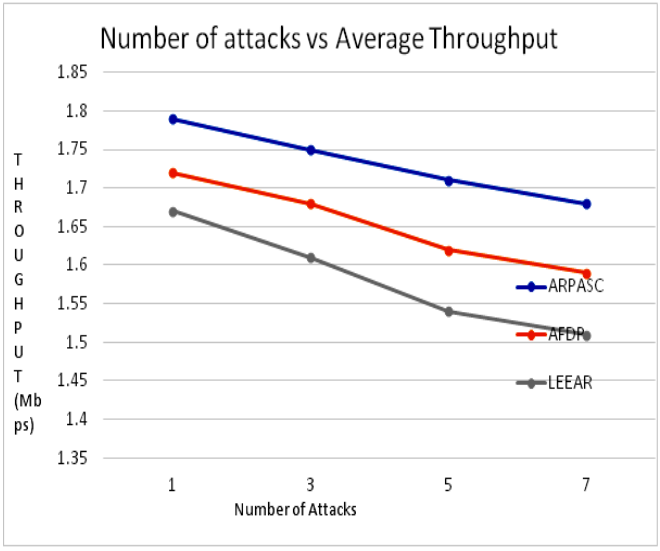

Fig.2.3 Throughput Vs Attacks

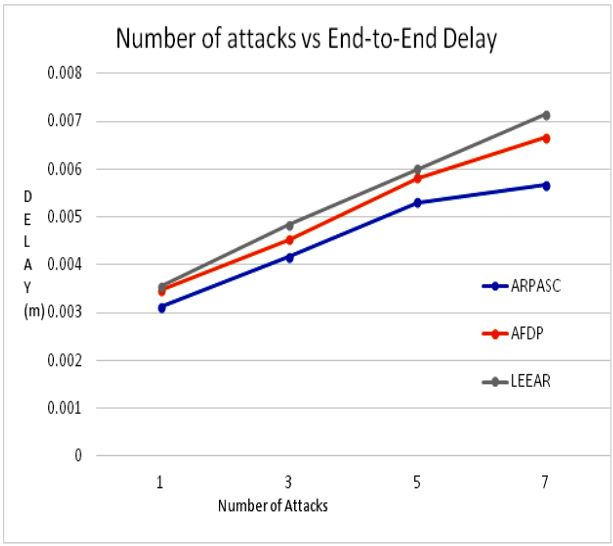

Fig.2.4 End to End Delay Vs Attacks

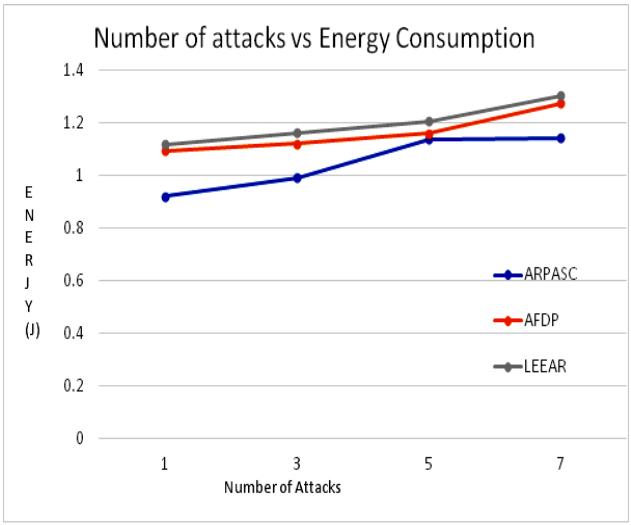

Fig.2.5 Energy Consumption Vs Attacks

IV. CONCLUSION

The advancement of protocols and cryptographic techniques deployed in MANET facilitates secured communication at lower cost. The efficiency of proposed protocols is measured in terms of packet delivery ratio, throughput, energy consumption and end to end delay. It can be concluded from the simulation results that the proposed protocols are 11%-14% more efficient than existing protocols. It can be concluded than the AFDP protocol is 6% - 8% efficient than LEEAR protocol. Simulation results show that the ARPASC protocol is 12% - 15% efficient than LEEAR protocol and 8% – 11% efficient than AFDP protocol.

REFERENCES

1. Kong, J., Hong, X., &Gerla, M., " An Identity-Free and On-Demand Routing Scheme in opposition to Anonymity Threats in Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol 6 , no 8, pp: 888-902, 2007.
2. Boukerche, Khatib, K. E., Xu, L., &Korba, L.,"SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Network", The twenty ninth Annual IEEE International Conference on Local Computer Networks, Tampa, Florida, USA, 2004.
3. Defrawy, K. E., &Tsudik, G.,"ALARM: Anonymous place supported directing in suspicious MANETs", IEEE Transactions on Mobile Computing, Vol10 no 9, pp:1345–1358, 2011.
4. Zhang, Y., Liu, W., and Lou, W.,"MASK : Anonymous on-request steering in transportable mainly appointed structures", IEEE Transactions On Wireless Communications, Vol five, no 9, pp: 2376–2385, 2006.
5. Goldwasser, S., Micali, S., &Rackoff. C.,"Knowledge Complexity of Interactive Proof Systems", Proceedings of STOC, pp: 291-304, 1985.
6. Heesook, C., William, E., Jaesheungn, S., Patrick, D. M., and Thomas, F. L. P.,"ASR: Anonymous and Secure Reporting of Traffic Forwarding Activity in Mobile Ad HoC

January-February 2020
ISSN: 0193-4120 Page No. 8276 - 8281

Networks", Wireless Networks, pp: 525 – 539, 2009.

7. Hsieh, W., &Leu, J.,"Anonymous validation convention depending on elliptic bend Diffie-Hellman for far off get admission to structures", Wireless Communications and Mobile Computing, Vol14, no 10, pp: 995-1006, 2012.
8. Abdul, S., and Gupta, K., "E-SHARP: Enhanced proven various leveled unknown directing convention for MANETs", International Journal of Computer Applications, Vol 153, number 1, pp: 17–20, 2016.
9. Shen, H., and Zhao, L., "ALERT: A mysterious place based totally proficient directing convention in MANETs", IEEE Transactions On Mobile Computing, Vol12, no 6, pp : 1079–1093, 2013.
10. Liu, W., and Yu, M.,AASR, "Confirmed unknown comfy directing for MANETs in adverse situations", IEEE Transactions On Vehicular Technology, Vol63, no nine,pp: 4585–4593, 2014.
11. Shabut A, Dahal K, Bista , Awan I , " Recommendation based trust model with a successful guard plot for MANETs.", IEEE Transactions on Mobile Computing,Vol14 ,no 10,pp 2101–2115, 2015.
12. GayathriDhananjayan and JanakiramanSubbiah, " T2AR: believe- conscious adhoc steering conference for MANET",SpringerPlus ,5:995,2016.
13. Larry A. Dunning, Member, IEEE, and Ray Kresman , "Protection Preserving Data Sharing With Anonymous ID Assignment", IEEE Transactions on Information Forensics and Security, Vol. Eight, no. 2, pp 402-413,February 2013.
14. Ziming Zhao, Hongxin Hu, Gail-JoonAhn, and Ruoyu Wu, "Hazard Aware Response for Mitigating MANET Routing Attacks", IEEE Transactions on Dependable and Secure Computing , Vol 9 , no 2 , March-April 2012..
15. Saini Das, ArunabhaMukhopadhyay, DebashisSaha& Samir Sadhukhan, "A Markov-Based Model for Information Security Risk Assessment in Healthcare MANETs", Springer Science+Business Media, LLC 2017.
16. A.Naveena, Dr.K.RamaLinga Reddy, "Vindictive Node Prevention and Mitigation in MANETs utilizing A Hybrid Security Model", distributed in Information Security Journal: A Global Perspective, e-ISSN: 1365-2575 ,Vol 27, Issue 2 ,pp: ninety two-one hundred and one, March-2018.
17. Network test gadget <http://www.Isi.Edu/nsnam/ns.