International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-1, November 2019

Enhancement of Security in Flying AD-HOC Network Using a Trust Based Routing Mechanism

Deepak Sharma, Aaisha Jameel

Abstract: ***Security is one of the most vital aspect for implementing FANETs in adverse environments. Hence, research in this area has emerged as an important FANETs field in the recent past. Compared to wired networks, FANETs are more vulnerable to security attacks due to lack of a trusted centralized authority and easy eavesdropping. Further, as nodes in flying ad-hoc networks are susceptible to attacks, a trust model based on direct, as well as indirect trust degrees from similar trusted neighbors is integrated in order to overcome the vulnerability due to attacks by malicious/selfish nodes and to provide reliable packet transmissions. Fading away of trust is incorporated with a perspective to ensure the uncertainty of trust with time until it is updated. Also, AODV algorithm is used for routing in combination with calculated trust values so that efficient transmission of messages can take place.***

Keywords: Mobile Adhoc Network (MANET), AODV Protocol, FANET, Network Security.

I. INTRODUCTION

In this chapter we are focusing on the basic introduction of FANET and routing protocols. Flying Ad-Hoc Network (FANET), which is basically ad hoc network between UAVs. FANET is one of the most effective ways to relay the collected information to the ground station without any infrastructure. UAVs are used in search for the people lost in forest, search and rescue, geo-mapping, firefighting, law enforcement, scientific research, crop management, surveillance of natural calamity hit areas etc. However, there are still many open issues about FANETs, such as security problem, finite transmission bandwidth, abusive broadcasting messages, reliable data delivery, dynamic link establishment and restricted hardware caused processing capabilities, maintaining efficient UAV to UAV communication, routing between UAV to UAV. The utilization of FANETs for various military, regular citizen, and business applications is required to convey great outcomes as far as dependable and deferral bound information conveyance. Movement checking, remote detecting, outskirt reconnaissance, fiasco administration, social insurance observing, and hand-off systems are a few zones where FANETs will be utilized. In reconnaissance applications, for example, fringe watch frameworks and urban observation, UAVs assume a vital part in limiting human mediation. UAVs that can screen and report occurrences or activity administration information are a monetarily and socially doable alternative as they don't require travel over streets. Besides, because of UAVs' high speeds, critical occasion particular information can be exchanged to help inquiry and safeguard missions. Territories, for example, woods and marshlands, which are difficult to reach by ground vehicles because of their remote areas, can be shielded from debacles, for example, out of control fires by remote sensor systems (WSN) and UAV systems.

The main objective of the proposed approach is the calculation of trust values of nodes present in FANET. By calculating trust of the nodes, we can detect malicious nodes present in the network which causes packet drops hence degrading the performance of the network. Once the malicious nodes are detected and removed, the transmission of data packets takes place through genuine and benevolently behaving nodes only. This in turn increases the security of the network as no malicious nodes are present or are being used for message transmission in the network.

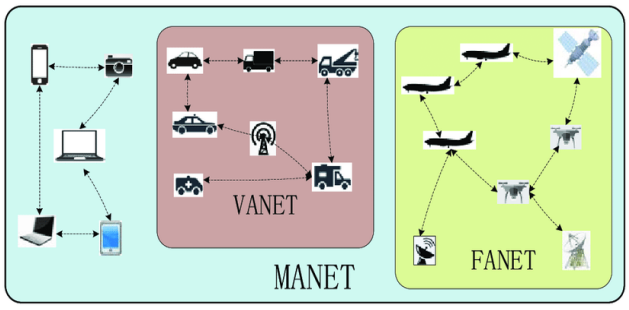

Fig. 1. MANET, FANET, VANET

II. LITERATURE REVIEW

In this chapter, we specifically focus on the existing work done in the respective field and some basic overview about the Flying Ad-hoc Networks. Security is one of the most vital issues in any network where the transmission of sensitive or important data might take place. FANETs being a wireless network comprising of a number of nodes are more prone to being attacked from outside sources which in turn brings the security into question. Hence, it needs to be taken care of very efficiently.

Revised Manuscript Received on November 30, 2019.
***** Correspondence Author
Deepak Sharma*, Ph.D, Research Scholar, Department of Computer Science, M. D. University, Rohtak., India. Email: erdeepaksharmabwn@gmail.com
Aaisha Jameel, PG student, CDAC, IP University, New Delhi, India. Email: aaisha.jameel01@gmail.com

Ilker Bekmezci et al. [3] analysed some Flying Ad-Hoc Networks which are an ad-hoc network connecting the UAVs. The points where FANETs, MANETs and VANETs are enlisted first and then the main FANETs design challenges are introduced. In addition to the existing FANETs protocols, open research problems are also discussed. The plus points of the multi-UAV systems are cost, scalability, survivability, speed up etc. The procurement and operational support cost of small UAVs is much lower than that of the large UAVs. The utilization of large UAVs lets only limited amount of coverage increase. On the other hand, multi-UAV systems can escalate the scalability of the operation effortlessly. If the UAV fizzles in a mission which is carried out by a single UAV, the mission cannot proceed. Whereas, if a UAV goes offline in a multi-UAV network, the mission can proceed with the other UAVs. It is very evident that the missions can be finished comparatively faster with more number of UAVs. Instead of having one huge radar cross section, multi UAV systems deliver very small radar cross sections, which is significant for military applications.

Sumathy Subramaniam et al. [4] proposed an improved trust model in light of the historical backdrop of past associations of both direct and suggestions from the trusted neighbors are utilized as a part of the calculation of the trust in degree. While the previous depends on coordinate communications, the last relates to the suggestions got by comparative and trusted neighbors. Comparable neighbors come into the photo as it is properly accepted that nodes that have comparable trust degrees on another neighbor as well. Once the trust degrees are set, just the nodes that fulfil a pre-decided limit esteem are utilized for packet transmission. This paper proposes another metric, for the determination and prioritization of competitors with the point of enhancing the lifetime of the system considering the lingering battery energy of every node in the connection and with dependable nodes as potential forwarders in the system. The trust module is in charge of the disposal of pernicious and egotistical hubs. It depends on both immediate and aberrant trust (utilizes two variables, closeness and direct trust) degrees. It mulls over the way that confide in blurs (winds up unverifiable) with time. The immediate trust degree, Td (i,j), that hub i has on hub j depends on the immediate cooperation between them previously. The way that trust blurs with time is thought about. The rot factor is characterized to such an extent that the trust on a node approaches the esteem 0.5 rather than the esteem 0 with time. This approach is more appropriate as the trust on a node ends up unverifiable with time until the point when it is refreshed straightaway.

Mentari Djatmiko et al. [1] proposed a novel probabilistic node choice model which gives a heap adjusting inside the number of inhabitants in nodes. Thus, a node's likelihood for being chosen for a cooperation will relate to its trust esteem. Moreover, it gives obscure nodes the chance to be chosen, in this manner empowering these nodes to add to the group. Here, they have accepted that in impromptu substance appropriation systems, nodes download the required substance from their prompt remote neighbors and consequently every one of the correspondences are single jump. Besides, we expect that all neighbors have the required substance and that substance is sub-partitioned into a few pieces. We propose Real Time Trust (ReTT), a novel dispersed trust assessment component that ceaselessly assesses trust amid an association. The component depends on the presumption that a collaboration between two nodes will comprise of various advances which can be separately investigated progressively. Figure demonstrates an outline of the proposed component. ReTT presents two choice focuses, the choice to interface with a node (choice to begin) and the choice to remain associated after the connection has begun (choice to proceed). The term constant mirrors the thought that recently got data is promptly assessed to frame a developing assessment of trust.

Dilraj Singh et al. [2] Cryptographic based Models Security in this approach is furnished with the utilization of cryptographic systems, for example, Symmetric or Asymmetric encryption and advanced marks. They can effectively give solid validation and approval base alongside protection from non-disavowal and non-flexibility of data. Be that as it may, these systems cause a lot of computational and vitality overhead which isn't wanted in MANETs because of asset rare hubs. Distributed Public-Key based Models If there should be an occurrence of Distributed Public-Key approach the thought is to make utilization of limit cryptography to convey the mystery key of the Certification Authority over various hubs which are characterized as servers. A subgroup of N server hubs out of aggregate hubs joins their fractional keys to create a mystery key.

This plan gives a hearty arrangement as the assailant hubs should overcome of all the N hubs to access the key after which it can bargain the system security. However, this approach requires certain level of pre-setup which challenges the fundamental contract of the MANETs. Notwithstanding this it expends significant measure of assets to keep this procedure working in a secure way.

The Distributed Trust based approach influences utilization of trust in the same as the individuals to use in their everyday exercises. According to this approach conventions have components to compute, prescribe and pull back trust for taking part hubs. Every hub needs to keep up its database to hold the trust esteems which are processed from immediate or backhanded assets.

It utilizes trust classes and confide in qualities to discover diverse levels of trust. This approach however is very adaptable to actualize and does not require any disconnected contact between hubs which clears bolster the dynamic idea of MANETs, it has a few disadvantages. Like, malevolent hubs can intrigue to ouster an honest to goodness hub by spreading false or one-sided proposals.

As the emphasis is chiefly on the idea of trust from the viewpoint of FANETs there are sure properties of confide in, Subjective, Asymmetric, Dynamic, Transitive, and Context Dependent. So Depending upon the properties of the trust represented while outlining of a trust show the accompanying contemplations must be thought about Decentralization, Customizable, Non-Cooperative nature, Self-Organization.

A trust show alludes to an applied reflection on which to assemble components for appointing, refreshing and utilizing put stock in levels between the substances in a circulated framework. So it can be determined that in given situation the trust show is an apparatus which helps the specialists in a disseminated framework to find dependable companions to play out its assignments.

Su Bing et al. [5] proposed efficient encryption mechanism is a trusted-based Algorithm combining the cryptographic encryption with the simple bit operation. The algorithm is implemented over the Dynamic Source Routing (DSR) protocol. Every node is given a number trust esteem lying between - 1 and 4. A trust of 4 characterizes an entire trust and a trust of - 1 characterizes a total doubt. The procedure is that a node with a trust level of x is given at most x parts of the bundle to forward. These trust levels likewise characterize the most extreme number of parcels which can be directed by means of these nodes. This constrains the likelihood of a savage power decoding of the message. A node with full trust or with a trust level of 4 can read the message.

A node with confide in level of 3, 2, 1 can read a few sections of message. A node with a trust level of 0 isn't given any parts of messages. A node of a trust level of - 1 is an ensured malevolent node and means that any bundle originating from that node ought to be dropped. No parcel is thusly steered to these nodes, prompting a disconnection of malevolent nodes. The trust level allotted to a node is a blend of direct association with its neighbors and the suggestions from its companions.

A node doles out an immediate trust level to its neighbor based on affirmations got. On the off chance that the neighbor sends an incite affirmation of the bundle got, it is accepted that the node isn't associated with an asset escalated savage power assault and consequently is doled out a higher trust level. The immediate trust is then joined with the trust proposal from its associates and a last trust level is allotted to it. Note that these trust levels are doled out progressively and are reserved by a node for execution upgrade.

III. PROPOSED APPROACH

In the current chapter, we will present an approach for calculating the trust of the nodes present in the network hence trying to enhance security of the FANETs.

A. Idea behind the Approach

The proposed approach defines a mechanism using which trust of the nodes present in the network can be calculated. In FANETs, due to wireless connections present between the nodes data is always at a risk of getting compromised by malicious nodes. These nodes are generally present externally with respect to the network, but there are very high chances that a number of nodes already present in the network may be corrupted or may get corrupted gradually over time. Hence, detection and removal of such nodes is the major concern of this approach. Before protecting the network from external attacks, it is very important to protect the network from internally compromised nodes. As the nodes in the FANET are moving at a very high speed, the trust values needs to be calculated, checked and updated really fast.

B. Working principle

All the nodes that form the network are assigned a default trust value of 0.5 by their neighbor nodes. The range of the trust value varies between 0 and 1. The threshold value of trust is set to be 0. Nodes above the specified threshold trust value of 0 are considered trustworthy or benevolent nodes. Any node that reaches or exhibits a trust value 0 will be immediately labelled as a malicious node and would be disconnected from the network. Every time a node successfully forwards a data packet to the intended node, its trust value gets incremented by 0.001. Similarly, when a node drops a packet it had to forward further, the trust value of that node gets decremented by 0.001. Routing/data transmission is performed only through trustworthy nodes. The trust table is updated regularly to keep a check on all the nodes present in the network.

C. Flow charts

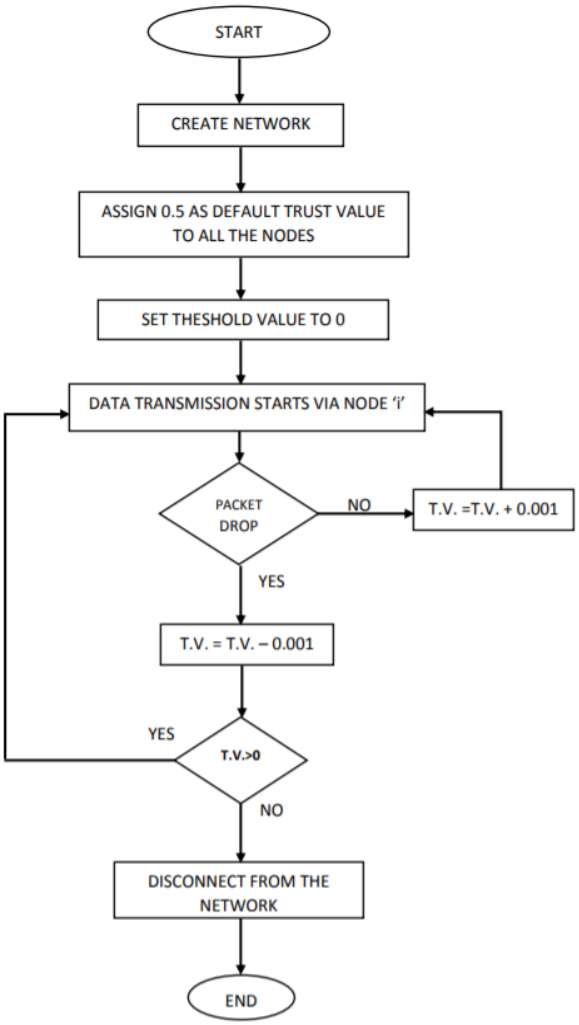

Fig. 2. Implementation of Cooperative Black Hole node

IV. IMPLEMENTATION AND RESULTS

This section focuses on the simulation and implementation of the proposed approach in an artificial environment created with the help of a simulation tool. The approach has been tested and verified.

A. Simulation environment

In Network Simulator for performing simulation we need to write down the TCL file. In order to run the simulation every time, we need to execute the command “ns” followed by the file name in the terminal available in the network simulator. Trace files are used to store all the detailed description about the traffic flow in the network.

It stores all information about nodes present and data transmission in the network. The file written by an application (or by the Coverage Server) to store coverage information or overall network information.

Table- I: simulation environment

Simulator	Network Simulator 2.35
Simulation duration	150 s
Data rate	1Mbps
Number of nodes	30
Data traffic type	TCP
Data payload	512 Bytes/packet
Simulation Area	800 m X 800 m
Routing Protocol Modified	TAODV
Transport Agent	UDP
Packet Format	CBR

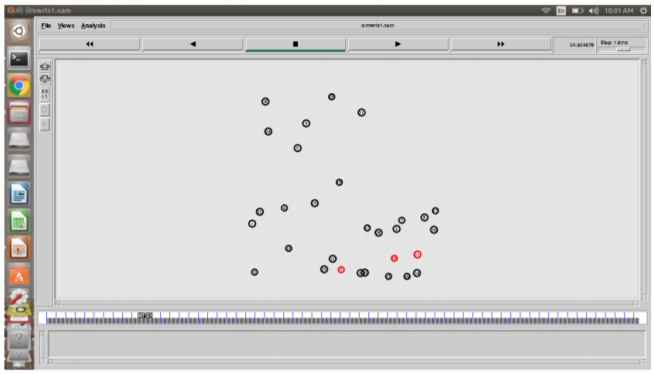

Fig. 3. Simulation result in NAM

B. Analysis using Trace file

Table- II: Format of Trace File [7]

Event	Time	Source Node	Layer	Flag	Dest. Node	Pkt type	Pkt size	Flags

Event shows the event that has occurred. Here's' represents send, 'r' represents received, and 'D' represents dropped packets. Time shows the time at the event has occurred. Source node holds the node id of the source node. Layer shows the layer at which the event has occurred. Destination node holds the node id of the destination node. Sequence of packets shows the sequence number of packet being transmitted. Packet type shows the packet type. For example 'CBR' packet, 'DSR' packet, 'MAC' packet generated by the MAC layer, 'ARP' packet generated by link layer. Packet size shows the size of the packet being transmitted. Flags shows flag symbol.

Table- III: Trace file results relevant to the proposed approach

D	0.553287992	0	RTR	MAL	0	CBR	532	13a 0 1 800	-------	1:0 2:0 29 0
D	0.562105786	0	RTR	MAL	3	CBR	532	13a 0 1 800	-------	1:0 2:0 29 0
D	0.562105786	0	RTR	TTL	0	TCP	0	0 0 0 0	-------	0:0 0:0 0 0
D	0.001131478	4	MAC	COL	0	TAODV	102	0 ffffffff 1 800	-------	1:255 -1:255 1 0
D	0.002482657	8	MAC	COL	0	TAODV	102	0 ffffffff 1 800	-------	1:255 -1:255 1 0
D	0.560153074	0	RTR	MAL	0	CBR	532	13a 0 1 800	-------	1:0 2:0 29 0
D	0.724336976	0	RTR	MAL	5	CBR	532	13a 0 1 800	-------	1:0 2:0 29 0
D	0.750874053	0	RTR	MAL	6	CBR	532	13a 0 1 800	-------	1:0 2:0 29 0

C. Results and comparison

Table- IV: Comparative Analysis: TAODV vs. AODV

No. of packets generated	Protocol	No. of packets received	Packet Delivery Ratio (PDR)
301	TAODV	156	51.82%
301	AODV	120	39.86%

Table- V: Comparative Analysis: TAODV vs. AODV

No. of packets generated	Protocol	No. of packets received	Packet Dropping Ratio (PDR)
301	TAODV	145	48.17%
301	AODV	120	60.13%

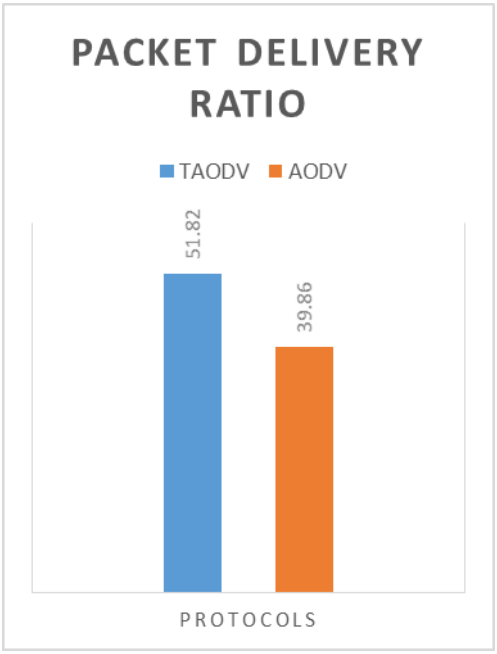

Fig. 4. Packet Delivery Ratio (PDR): TAODV vs. AODV

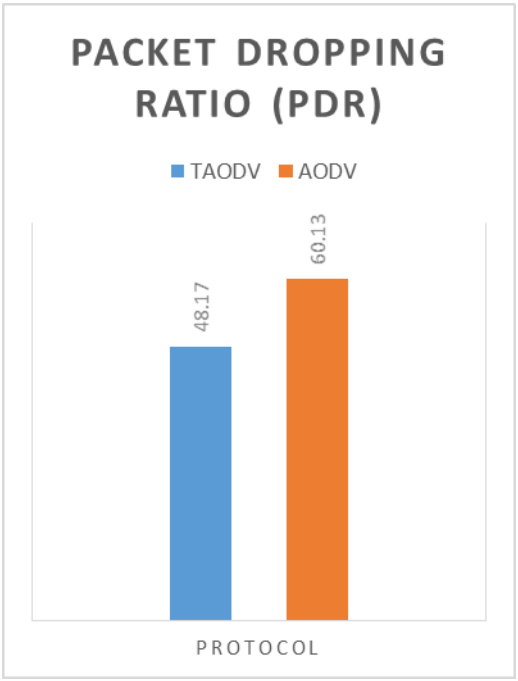

Fig. 5. Packet Dropping Ratio: TAODV vs. AODV

V. CONCLUSION AND FUTURE SCOPE

In this chapter, we will discuss what we have achieved after doing this work and how it will be helpful in future endeavors.

A. Conclusion

After the completion of the mentioned project, we can calculate the trust value of various nodes present in the network. Based on the calculated trust value of the node and the threshold trust value that we have set for a node to be labelled as malicious or trustworthy, we can further decide whether to keep the node in the network or disconnect it. Node that falls under the category of malicious nodes is disconnected from the network and not used for any further routing or message transmission. The network becomes secure or threat free due to the removal of malicious nodes.

B. Future Scope:

This approach focuses on enhancing the security of a network through the detection and removal of malicious nodes in the network. This approach was tested on a small number of nodes. Security of the system can be improved through many other perspectives as well. This approach does not aim at the security of the data packets that are transmitted. • The data packets can be encrypted using a strong encryption algorithm, like AES-256 which is generally known to be the golden encryption standard.

REFERENCES

1. Mentari Djatmiko, Roksana Boreli, Aruna Seneviratne, Sebastian Ries, “Trust Based Content Distribution for Mobile Ad Hoc Networks” in 2011 IEEE 19th Annual International Symposium on Modelling, Analysis, and Simulation of Computer and Telecommunication Systems.
2. Dilraj Singh, Amardeep Singh, “Trust Based Routing Protocols in Mobile Ad Hoc Networks” in 2014, 4th IEEE International Conference on wireless communications, networking and mobile computing.
3. Ilker Bekmezci and Ozgur Koray Sahingoz and Samil Temel, “Flying Ad-hoc Networks (FANETs): A survey” in Ad Hoc Networks journal, vol. 11, pp. 1254-1270, Jan 2013.
4. Sumathy Subramaniam, R. Saravanan and Pooja K. Prakash, “Trust Based Routing to Improve Network Lifetime of Mobile Ad Hoc Networks” in Journal of Computing and Information and Technology, Volume 18, Issue 5, October 2013, pages 666-677.
5. Su Bing, Ma Zheng hua and Sun Yu-qiang, “A trusted based encryption mechanism for efficient communication over wireless networks”, in 2008, 14th IEEE International conference on Computer Science and Technology and Cloud Computing.
6. http://www-rp.lip6.fr/ns-doc/ns226-doc/html/aodv_8cc_source.htm\
7. http://www.cs.binghamton.edu/~kliu/research/ns2code/
8. C. E. Perkins and E. M. Royer, “The ad hoc on-demand distance vector protocol,” in Ad hoc Networking, Addison-Wesley, pp. 173–219, 2000.
9. S.Bhimla, N.Yadav,”Comparison between AODV protocol and DSR protocol in MANET”, IJAERS, Vol 2, issue 1, 2012.
10. https://www.researchgate.net/figure/Figure-FANET-Applications-In-Sensor-NetworksDifferent-sensor-devices-can-be-used-to_fig1_317446275.

AUTHORS PROFILE

Deepak Sharma, is currently pursuing a Ph.D. in Computer Science at M. D. University, Rohtak. He has completed his M.tech from C-DAC: Centre for Development of Advanced Computing, Ministry of Communications and Information Technology, Government of India affiliated from Guru Gobind Singh Indraprastha University, Delhi. His main research areas include Data mining, Mobile Adhoc Network (MANET), wireless sensor network (WSN) and Internet of things (IoT).

Aaisha Jameel, has successfully completed her master's degree in computer science and engineering from C-DAC, Noida affiliated to Guru Gobind Singh Indraprastha University, New Delhi. Her research dimension covers computer networking and network security.