ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

Introduction to variations of MANETs: VANETs and FANETs

Dr Ashish Khanna, MAIT, GGSIPU, Delhi, India, ashishk746@yahoo.com

Abstract: Mobile Ad-Hoc Networks are self-ruling and decentralized remote frameworks. In Mobile Ad-hoc Networks (MANET), every dynamic node goes about as a host and also like a router. The nodes impart to each other by communication of hop-to-hop. [1] The dynamic nature of MANET permits nodes to join and leave the system at any time. Nodes are the frameworks or devices i.e. cell phone, tablet, personal digital assistance, and PC that are partaking in the system and are portable. MANET which using wireless is especially helpless because of its principal qualities, for example, open medium, dynamic topology, appropriated collaboration and obliged ability. Thus, security in MANET is a mind-boggling issue.

Introduction

In MANETs key and trust management is a basic supporting component in any of the security frameworks. Its fundamental operations incorporate the building up key swap and amend, and also secret associations. Keys are the essential squares of symmetric and asymmetric cryptographic capacities, which thus outfit confirmation, privacy, uprightness, and non-repudiation security services. The security in systems administration is as a rule subject to appropriate key management. Management of the Key comprises of different administrations, of which each is crucial for the networking system's security.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

Trust model: it must be resolved how plenty of different components in the system can believe each other. Subsequently, the trust connections between system components influence the way the key management framework is developed in system.

Trust third party (TTP): [2] a centralized authority (e.g., a key distribution center [KDC] or certification authority [CA]) is trusted by each substance and an element A is trusted by another if the authority claims A is dependable.

Web-of-trust [3]: There is no specific structure exists in such trust charts. Every element deals with its own trust in light of direct suggestion from others.

Localized trust: [4] this model is the center ground of the past two diagrams. A node is trusted if any k trusted substances among the node's one-hop neighbors assert along these lines, inside a limited time period.

Cryptosystems: accessible for the key management, at times just public or symmetric key techniques can be achieved, while in different settings Elliptic Curve Cryptosystems (ECC) are exists. Even though public key cryptography offers more comfort. Public key cryptosystems are somewhat slower than their secret key partners when comparable level of security is required.

There are bunches of trusted models and protocols for routing which are utilized as a part of MANETs to accomplish security. Distinctive trust methods are utilized to give privacy, uprightness and accessibility in mobile ad-hoc network to pick up the safe environment. Supplying trust in MANET is an extra basic errand due to absence of centralized infrastructure. After all, amid the setting out of MANET nodes that are crisp

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

keep returning and matured ones go from the cluster/network, there is interest for keeping up the record additionally to give proper affirmation to the arriving node(s) that are new and in addition the present node(s) in the system. In this paper, A review on different sorts of key management schemes with their unique elements is presented. Additionally, a review of MANET interruption discovery frameworks (IDS), which are responsive ways to deal with upset assaults and utilized as a moment line of protection is also proposed. [5] discussed about Reconstruction of Objects with VSN. By this object reconstruction with feature distribution scheme, efficient processing has to be done on the images received from nodes to reconstruct the image and respond to user query. Object matching methods form the foundation of many state- of-the-art algorithms. Therefore, this feature distribution scheme can be directly applied to several state-of- the-art matching methods with little or no adaptation. The future challenge lies in mapping state-of-the-art matching and reconstruction methods to such a distributed framework. The reconstructed scenes can be converted into a video file format to be displayed as a video, when the user submits the query. This work can be brought into real time by implementing the code on the server side/mobile phone and communicate with several nodes to collect images/objects. This work can be tested in real time with user query results.

2.1 FANETS

Unmanned Aerial Vehicle (UAV) systems, which can flyautonomously without carrying any human personnel, is aconsequence of quick development in communication andelectronic sensor technologies. Easy deployment, flexibilityand low functioning cost

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

of UAVs have expanded both thecivilian and military applications of it; such as bordersurveillance [1], search and destroy operations [2], relay for adhocnetworks [3,4], managing wildfire, remote sensing [6],traffic monitoring [7] and disaster monitoring [8]. Instead ofdeploying single UAV, which have been used for decades,using a network of UAVs(FANET) has many advantages suchas enables to survey a greater area, raises the scalability and lowers the maintaining effort.

When high-speed UAVs form the network structure of FANET, it becomes different from the existing ad-hoc networks like Mobile Ad-Hoc Network (MANET), Vehicle Ad-Hoc Network (VANET)[9] and Wireless Sensor Network[10] in terms of design and security issues. The higher mobility degrees of FANET nodes result in frequent topological change and unlike other ad-hoc networks the distance between the nodes in FANETs are longer while compared. Hence a fast group forming and key distributing protocol becomes mandatory for FANET while existing mechanisms [11, 12, 13] become ineffective due to the structure and manner of the network.

To cope with the manner of FANET with high speed nodes,a simple yet powerful group key establishment protocol isproposed in this paper. The proposed protocol facilitates groupestablishment among UAVs of high mobility degreeconcentrating on their security issues. Classification of wireless ad-hoc networks is doneaccording to their deployment, utilization, communication andpurposes. FANET fall under the subgroup of VANET, whichagain belongs to the subset of MANET. According to thisdefinition, a FANET cannot be formed with single UAVsystems, but only with multi-UAV systems. Again, multi-UAV systems cannot be named as FANET until thecommunication between UAVs

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

is realized by an ad-hocnetwork *i.e*. communications between UAVs must not fullyrely on infrastructure links.

Flying adhoc network (FANET) represents a particularly newclass of adhoc networks. FANET is allow to send informationquickly and accurately in a situation, where generic adhocnetworks are not capable to do so. At the time of naturaldisaster like flooding, earthquakes and even in militarybattlefield FANET can perform better than other form ofmobile adhoc networks [1]. FANET uses a group ofhomogenous flying agents called MAVs(Micro Air Vehicle)communicates with each other locally, and also interacts withtheir environment to get some sort of information. FANETs donot support central control system [2]. In FANET position ofMAVs changes rapidly and because of this, there are frequentchanges in topology. High mobility of nodes in FANET is a very bigissue, so here we have applied and analyzed OLSR inFANETs. Also try to find a mobility models through whichperformance of OLSR can be improved for FANET.The use of autonomous vehicles have increased in civiland military applications like observation, search and rescue,surveillance, and reconnaissance, etc. The main reason isthe desire to reduce human risk and increase mission efficiencywhen executing missions [1]. Autonomous vehiclescan be terrestrial (Unmanned Ground Vehicles - UGV), aerial(Unmanned Aerial Vehicles - UAV) and others which aregenerally controlled, managed and monitored in real timeby embedded systems, that have severe restrictions aboutfaults once it might cause human deaths and/or losing highvalue components. Then, these systems are known as criticalembedded systems.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

Another characteristic of this kind of vehicle is thatthey are able to function during a long period without theinterference of human's operators, and then they can makethe navigation basing on a grid or in a way-points sequence[2]. During the operation, these vehicles are subject to threatsthat might be fixed obstacles (e.g. walls, constructions, vegetation),or mobile (e.g. other vehicles, birds), and then theyhave to be able to detect them and realize evasive maneuvers.Yang et al [3] states that the major problem of obstacleavoidance can be divided in "sense" or "detection", that is the perception of the obstacle and; "avoidance" that meansrealize an evasive maneuver in order to avoid the obstacleand reestablish the programed route before the maneuver. Theauthors also highlight that this is one of the most challengingproblems in autonomous navigation field.Autonomous Vehicles might also form networks and collaborateamong them through the exchange of messages.

Thecommunication of these vehicles occurs through vehicular orfly networks. Currently three vehicular network architecturesare known: ad hoc pure (VANETs - Vehicular Ad hoc Network),generally used in V2V (Vehicle-to-vehicle) communications;the infrastructure way, used in the communication ofthe vehicle with a network infrastructure (V2I - Vehicle-to-infrastructure);and the hybrid approach, where the mixtureof the architectures ad hoc and infrastructure are used.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

VANETs : Vehicular Ad hoc Networks

Vehicular Ad hoc Network has a special subtype knownas FANET (Flying ad hoc network) that is an ad hoc networkcomposed by aerial vehicles. The FANETs has specialcharacteristics from when compared with another network.In FANETs the nodes have greater degree of mobility andhence the network topology changes frequently. Anothercharacteristic is that the distance between the nodes is oftenhigher than in VANETs [4].In the case of infrastructured networks (V2I), static nodesbehave as access points for IEEE 802.11 networks and havethe advantages of increasing connectivity and creating thepossibility of communicating with other networks, such as,the Internet. However, in infrastructured approach there isthe disadvantage of high cost in deployment of networkequipment to cover the entire route of the road. In somecases it is possible to reduce costs by deploying a third typeof architecture known as hybrid. This last one uses ad hoccommunication type associated with a minimal infrastructureto increase network connectivity in service provision.The choice of these model's architecture has to take intoaccount several factors such as the density of vehicles on theroad, obstacles in the path and the applications for whichthe VANET is proposed. There are three main applicationsof vehicular networks: traffic safety, entertainment and driverassistance. The increase of traffic safety is a major motivation for the use of vehicular networks, because it generally aims toreduce accidents by exchanging information among vehiclesand gathering information about the conditions of the roadby sensors.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

A. Network Architecture

The architecture of FANET can be organized inhierarchical and distributed structures as shown in Fig. 1.In hierarchical networks as shown in Fig. 1(a), there is achain of command among the UAVs: base stations, groupheads and member UAVs. A base station is typically apowerful storage / data processing center, gateway to anothernetwork, or works as a human interface. Base stations collectinformation from UAVs, carries out expensive operations andorganize the network. Base stations are considered to be trustedand temper resistant and register UAVs prior deployment.Group heads are deployed around the surveillance area each of which can act as a member under another group leader. Thisstructure allows UAVs to monitor a larger area beyond thetransmission range of the base station. Each leader maintains agroup comprising several member UAVs. Together withmembers a group leader monitors a pre-assigned area andtransmits data to the base station. Data collected by themember UAVs are transmitted through group leaders. Dataflow in such networks can be:

(i) pair-wise (unicast) amongmember UAVs,

(ii) group-wise (multicast) within a group ofUAVs, and (iii) network-wise (broadcast) from base stations toall UAVs.

Distributed architecture of FANET is illustrated in Fig.1(b) where, there is no fixed infrastructure and networktopology is unknown before deployment. UAVs spreadrandomly all over the surveillance area. Once deployed, eachUAV scans its coverage area to find out its neighbors. Dataflow in such network is similar to the data

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

flow in hierarchicalnetwork with a difference that network-wise (broadcast) can besent by every UAVs.

B. Distinguishing characteristics of FANET

In this subsection, the differences between FANET and theexisting wireless ad-hoc networks are explained which make itnecessary to propose a different group key managementprotocol.

Node mobility: The most notable dissimilarity betweenFANET and the other ad-hoc networks is node mobility.Unlike VANET and MANET, the node's mobility degree canbe much higher in FANET. UAVs may have a speed of 30–460km/h [14] which results several challenging problems incommunication design [15].

Mobility model: MANET nodes, moving on a certainterrain, generally apply the random waypoint mobility modelwhere the speed and the direction of the nodes are selectedarbitrarily. In VANET nodes mobility models are highlypredictable as their moves are restricted on roads andhighways. For FANET, though the preference of global pathplans in some multi-UAV applications forces UAVs to moveon a predefined path with a regular mobility model, flight plansare not planned in autonomous multi-UAV systems. Moreover,updates in operation or environmental changes always affectthe flight plans. In addition, different UAV formations and thesharp and fast movements of UAVs directly influence themobility model of FANET.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Issue 9, September 2017

Node density: The average number of nodes in a unit area isdefined as node density which is considerably low in FANET.FANET nodes are normally scattered in the sky with a distanceof several kilometers even for a small multi-UAV system.

Topology change: Unlike MANET and VANET, FANETtopology changes more frequently due to the higher mobilitydegree. Moreover, FANET topology is also affected by UAV platform failures. Failure of UAVs, also fails the links in whichthey were involved resulting in a topological update. Linkoutage is another factor that influences the FANET topologywhich is caused by frequent change of link quality with UAVmovements and variations of node distances

ConclusionFANETs, VANETs and MANETs are closely related areas with some of the fundamental differences. Lot of research is going in this domain

References

1. Yi, P., Dai, Z., Zhong, Y., Zhang, S.: Resisting Flooding Attack in Ad Hoc Networks. In:IEEE International Conference on Information Technology Coding & Computing, pp. 657–662 (2005).
2. Martin, T., Hsiao, M, Dong, H., Krishnaswami, J.: Denial-of-Service Attacks on BatteryPowered Mobile Computers. In: IEEE International Conference on Pervasive Computing andCommunications (PerCom) (2004).
3. Hsu, H., Zhu, S., Hurson, A. R.: LIP—a Lightweight Interlayer Protocol for Preventing Packet Injection Attacks in Mobile Ad Hoc Networks. In: International Journal of Securityand Networks, Vol. 2, Nos. 3/4, pp. 202–215 (2007).
4. Sarkar, M., Roy D. B.: Prevention of Sleep Deprivation Attacks using Clustering. In: IEEE ICECT, Vol. 5, pp. 391–394 (2011).
5.Christo Ananth, M.Priscilla, B.Nandhini, S.Manju, S.Shafiqa Shalaysha, "Reconstruction of Objects with VSN", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Vol. 1, Issue 1, April 2015, pp:17-20.
6. Medadian M., Yektaie M. H., Rehmani, A. M.: Combat with Black Hole Attack in AODVRouting Protocol in MANETs. In: IEEE Asian Himalayas International Conference onInternet (2009).

7. Zhang, X. Y., Sekiya Y., Wakahara, Y.: Proposal of a Method to Detect Black Hole Attack inMANETs. In: IEEE International Symposium on Autonomous Decentralized System ISADS(2009).
8. Xiaopeng, G., Wei, C.: A Novel Grey Hole Attack Detection Scheme for Mobile Ad-HocNetworks. In: IFIP International Conference on Network and Parallel Computing (2007).
9. Wei, C., Xiang, L., Yuebinand, B., Xiopeng, G.: A New Solution for Resisting Grey HoleAttack in Mobile Ad Hoc Networks. In: IEEE Conference on Communication and Networking, China (2007).
10. Yang, B., Yamamoto, R., Tanaka, Y.: Historical Evidence Based Trust Management Strategyagainst Black Hole Attacks in MANET. In: IEEE ICACT, pp. 394–399 (2012).
11. Sharma, H., Garg, R.: Enhanced Lightweight Sybil Attack Detection Technique. In: IEEEConfluence, pp. 476–481 (2014).
12. Abbas, S., Merabti, M., Jones, D.: Signal Strength Based Sybil Attack Detection in WirelessAd hoc Networks. In: IEEE DESE, pp. 190–195 (2009).
13. Tangpong, A., Kesidis, G., Hsu, H., Hurson, A.: Robust Sybil Detection for MANETs, In:IEEE ICCCN, pp. 1–6 (2009).
14. Hashmi, S., Brooke, J.: Towards Sybil Resistant Authentication in Mobile Ad hoc Networks.In: IEEE Secureware, pp. 17–24 (2010).
15. Hu, Y., Perrig, A., Johnson, B.: Rushing Attack and Defence in Wireless Ad Hoc NetworksRouting Protocol. In: ACM Workshop on Wireless Security, pp. 30–40 (2003).