International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

Improved Security and Efficient Routing With Mesh Networks

N.Savitha
Assistant Professor, Department of Computer Science
University College for Women, Koti, Hyderabad.

Abstract: In an unforeseen event causing great loss need of some UAV's to surmount the destroyed network. On demand network admittance and penetration of sized areas of network done thoroughly in WMN. Attacks on network and security in the wireless network are major challenges. Here, presenting the position-aware, secure, and efficient mesh routing approach (PASER). The proposal prevents more attacks than the IEEE802.11s/i security mechanisms and the well-known, secure routing protocol ARAN, without making restrictive assumptions. In realistic UAV-WMN scenarios, PASER achieves similar performance results like, routing protocol HWMP combined with the IEEE 802.11s security mechanisms. Furthermore this system implemented is to propose a Channel-aware Reputation System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs. The CRS-A evaluates the data forwarding behavior of sensor nodes, according to the deviation of the monitored packet loss and the estimated normal loss.

Keywords- Wireless mesh networks, secure routing, routing attacks, IEEE 802.11s, IEEE 802.11i, PASER

I. INTRODUCTION

The report indicates that one of the top concerns in disaster areas is the disruption of telecommunications. In this context, Sugino reports, in a summary of the damages of the great east Japan earthquake and tsunami in March 2011, that million fixed telephone lines and 29,000 cellular base stations were damaged. He also reveals that emergency restoration of communication networks took one month, while a full restoration took 11 months. These facts emphasize the increasing importance of portable communication networks in disaster areas. Moreover, these figures point out that a communication network that does not rely on existing infrastructure and that can be deployed in a substantially short period (e.g., one hour) is indispensable to efficiently cope with large-scale crises. Low altitude, autonomous Unmanned Aerial Vehicles (UAVs) acting as WLAN or LTE aerial hotspots meet these requirements. Additionally, the UAVs can be equipped with sensors for cooperative exploration of scenarios where uncontrolled emissions of liquid or gaseous contaminants exist. UAV-assisted applications also include coverage extension/densification, precision farming, and polar weather monitoring. Nevertheless, for such applications to become a reality, a reliable, auto-configuring, and self-healing wireless backbone network is needed to interconnect the UAVs and to provide a connection to their ground control station, the Internet, and the cellular core network. Wireless Mesh Networks (WMNs) are a good candidate as they have the aforementioned characteristics, and they offer a physical air-toair link for a direct communication between the UAVs. illustrates how an airborne mesh network consisting of UAVs connected via a WMN (UAVWMN) can be used to assist in disaster relief operations. As the figure shows, the UAVs build a portable wireless mesh backbone. This backbone offers, on demand, network coverage to legacy mobile WLAN/LTE clients (rescue fighters' devices). It also deals with the transparent delivery of the clients' data as well as the sensor information of the UAVs. The surveys present a comprehensive analysis of the security in WMNs. They point out that several attacks are common in wireless networks such as jamming at the PHY layer, and these can be mitigated by conventional security

mechanisms, while some attacks are specific to WMNs. The latter mainly includes attacks on the core service of the mesh backbone, which is routing, such as the wormhole and black hole attacks, and user-related attacks, e.g., attacks on the user privacy with respect to data content, traffic flows, and location.

In this research, we focus on the security of the routing functionality. For privacy preservation and other user-related security services in WMNs, several approaches have been proposed which can be applied in combination with secure routing. For instance, in disaster scenarios, end-to-end security mechanisms are already used to ensure the privacy of the data of rescue fighters, while the privacy of their traffic flows (source, destination) and their location are not really a concern as these information are predefined in their public regulations.

The complexity of the network deployment and maintenance, it makes the WMN backbone prone to routing attacks, including the wormhole and black hole attacks. Consequently, an attacker can, with little cost or effort, redirect the traffic and drop the data packets even if the wireless backbone links are encrypted. In UAV-WMN-assisted disaster relief situations, this can sabotage the communication between rescue fighters. In addition, the data exchanged between the UAVs and their ground station will get disrupted. This issue makes the use of WMNs (or any wireless multi-hop solution relying on a routing protocol to dynamically set up routes) problematic for the command and control of the UAVs in practice as flight regulations impose that it should be always possible to remotely pilot the UAVs [11]. Thereby, the control of the UAVs is currently divided into two categories: The high level control of the whole UAV swarm via the operator (the ground station) and the direct control of each UAV via a safety pilot, which burdens pushing UAV-WMN to a wide scale deployment.

The emergence of airborne network-assisted applications in disaster relief, they are key solutions for 1) on demand ubiquitous network access and 2) efficient exploration of sized areas. Nevertheless, these solutions still face major security challenges as WMNs are prone to routing attacks.

Consequently, the network can be sabotaged, and the attacker might manipulate payload data or even hijack the UAVs. A wireless mesh backbone composed of mobile (UV) nodes and a static (ground station) node. The network is operated by one organization which restricts the access to the network.

Legitimate operator nodes conform to the system protocols while malicious nodes might deviate from them. A public key infrastructure is assumed, with the network operator playing the role of the certification authority. Legitimate nodes have a certificate with integrated roles. The network operator runs a secure Key Distribution Center (KDC) that is responsible to dynamically manage network credentials. All the nodes know the public key of the KDC. At any time, mesh gateways can establish a reliable connection to the KDC and vice versa. In UAV-WMN, this can be realized by running the KDC at the ground station. The efficiency of PASER is explored in a theoretical and simulation-based analysis of its route discovery process, and its scalability with respect to network size and traffic load is reason

II. RELATED WORK

We refer approach to reinforce the correspondence arrange against future debacles. After the quake, the talk has proceeded, and incorporates another critical point of convergence of how to take compelling measures in regular daily existence. This discussion will talk about the effect of the seismic tremor and the torrent on Japan's media transmission organize, advance in its recuperation endeavors, and also activity arrangements and R&D strategy towards building reliable future system framework [1].

From late innovation systems made out of numerous UAS and ground stations, alluded to as UAS-helped

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 03 Issue 13
September 2016

correspondences systems, presently can't seem to get adequate research consideration. In this paper, we address a major research challenge hindering such systems, which is the means by which to decently augment the vitality productivity (throughput per vitality) in systems including versatile adjustment able ground hubs. For the versatility design characteristic for the UASs, we show how versatile adjustment is influenced. Besides, we figure the issue of expanding reasonable vitality effectiveness as a potential amusement that is played between the numerous ground hubs and substantiate its security, optimality, and joining. Broad reproductions display the viability of our proposition under changing situations [2].

To augment the volume of air inspected by the UAVs amid an individual testing mission, the introduction interim must be as short as could be expected under the circumstances. The paper gives a basic, geometric strategy for producing hopeful time ideal ways in enduring winds, in light of Dubins' notable outcomes for least time ways of limited bend.

The approach is utilized to create ways for both UAVs, which must facilitate their movement along their individual ways keeping in mind the end goal to maintain a strategic distance from impact. The depicted techniques were tried amid an aerobiological inspecting test concentrating on the plant pathogen Phytophthorainfestans [3].

Because of exceptional qualities, for example, dynamic system topology, restricted transmission capacity, and constrained battery control, steering in a MANET is an especially difficult assignment contrasted with an ordinary system. Early work in MANET investigate has for the most part centered round building up an effective directing component in such a very unique and asset obliged arrange. At present, a few effective directing conventions have been proposed for MANET [4].

Multi jump remote specially appointed systems, portable hubs collaborate to shape a system without utilizing any framework, for example, get to focuses or base stations. Rather, the versatile hubs forward parcels for each other, permitting correspondence among hubs outside remote transmission go. The hubs' portability and on a very basic level constrained limit of the remote medium, together with remote transmission impacts join to make noteworthy difficulties for directing conventions working in a specially appointed system [5].

III. PROPOSED SYSTEM

System Architecture: The security in WMN is necessary having security at greater extent. The security is provided in the previous work with standards of security 802.11i/s. But these are unnecessarily not effective. These security standards need to use with effective routing protocols. Now in this work, the prevention of attacks routing overcome with this PASER using security mechanism like with the SEEHR Secure Energy Efficient Hierarchical Routing protocol and routing mechanism using DSR(Dynamic Source Routing). Thus these standards are used combined with security standards to prevent attacks from forgery. With the help of SEEHR, if the path between source and destination is busy or attacked then the offline path is created for packet transmission. Thus the energy of node to send packet is reduced. Modules used in this system explained below.

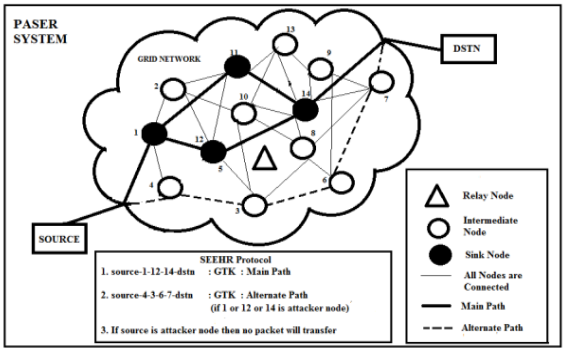

Fig.1 System Architecture of Proposed System

1) WSN formation with Mesh: In this module WMN is designed with network nodes interconnected

to each other's. It is good candidate network for air to air network for direct communication.

2) Route Discovery: Wireless network used for packet transmission from multiple sources to respective destinations. Here in this network communication bellman ford equation calculates shortest path network link. For network data downlink and uplink created. DSDV algorithm is used for shortest path. AODV is ad-hoc on demand distance vector routing protocol used for the routing of packet in network with the routing table stored at each node. It is store and forward concept.

3) Key Cryptography: The network nodes are assigned with secret key for secure wireless packet transmission. Random key generation algorithm is for producing network access keys. Asymmetric key Encryption is used for the key cryptography.

4) Key Authentication: At the time of packet transmission network nodes assumed to be verified for their assigned key if network access computed node is authorized to send packet across the network. GTK that is group transient key is used for secure communication. Node not having GTK acts as an attacker node in network default. SHA-256 algorithm for the key generation which gives hash values that are unique thus here also security of message is prevented.

Mathematical Model

1) Shortest Path Mechanism

Input is given as:

A graph with vectors and edges,

G = (V, E)

- The edges can be directed or not
- We grant negative edge weights

Output:

Two nodes A and B that reduces the total weight or cost length and path is created between them. Sometimes, we compute all-pair shortest paths. While sometimes, calculate shortest paths from A to all other nodes.

2) Destination Sequenced Distance Vector

Bellman Ford equation part of DSDV where each node has routing table and it is maintained which creates path which is shortest to respective destination node in the network. Multi-hops up to the destination produced. At each node to distinguish theft routes from new node and avoid from routing loops the sequence numbers are used. A new broadcast route contains,

- Destination Address
- Multi-hops for packet reception at the destination.
- Sequence number of the packet updated at each node to deliver at destination and a sequence number formed is unique to broadcast.

To maintain table consistency the routing tables updating done periodically. Each node has routing table that consists of information about destination address.

Graph:

G = {R, L}

R = set of routers,

{a, b, c, l, m, n}

L = set of links,

{(a, b), (a, l), (b, l), (b, c), (l, c), (l, m), (c, m), (c, n)}

3) DSDV Algorithm

Bellman Ford Equation given as, Dl(m) =Path cost from x to which is least then,

Dl(m) = min (C (l, b) + Dm(m)) …… (1)

Where D is Shortest Distance of X and Y coordinate and C is shortest path cost between two vectors.

Asymmetric Key Encryption: The encryption process where encryption and decryption done with two keys that are private and public. These different keys mathematically related gains the feasibility by cipher text decryption to get plaintext.

 User has public and private key. Encryption done by public key and decryption by private key.

 Public key broadcasted and private key is known to only that respective user. Hence, it is Public Key Encryption.

 It is impossible computationally in practice to find one from another. This is strength of this scheme.

 Host1 sends data to Host 2, he gets from storage public key of Host 2, data encryption by Host 2's public key and transmits.

 Host 2 to extracts the plaintext using own private key.

 Encryption has large key length thus encryption-decryption process is slower than Symmetric Key Encryption. Computer system need to run asymmetric algorithm is higher need to take care of power of processing.

IV. CONCLUSION

Proposed approach that is PASER protocol improves the drawbacks of existing system such that attacks vulnerability with 802.11i/s. The node security issues are overcome using SEEHR. To maintain the routing table security the AODV protocol used. Furthermore, the authentication while transmitting packet is achieved using GTK, Asymmetric Encryption and SHA-256 algorithm. Proposed implementation evaluates the system performance for channel aware routing to overcome path diversion during packet transmission. This helps to overcome warm hole and black hole attack in the network. Session wise digital signature is used along with public key cryptography for information security at end to end packet transmission.

REFERENCES

[1] European Commission. (2015). Flying New Way, RPAS, A Boost for European Creativity and Innovation [Online]. Available: http://ec.europa. eu/growth/flipbook/rpas/?goback=.gde

[2] United Nations (UN). (2015). Global Assessment Report on Disaster Risk Reduction [Online]. Available: http://www.preventionweb.net/english/ hyogo/gar/2013

[3] I. Sugino, "Disaster recovery and the R&D policy in Japans telecommunication networks," in Proc. Opt. Fiber Commun. Conf. Expo./Nat. Fiber Optic Eng. Conf. (OFC/OFOEC), 2012.

[4] J. Constine. (2015). Facebook Will Deliver Internet via Drones, TechCrunch [Online]. Available: http://techcrunch.com/2014/03/27/ facebook-drones/

[5] C. Wietfeld and K. Daniel, "Cognitive networking for UAV swarms," in Handbook of Unmanned Aerial Vehicles, K. P. Valavanis and G. J. Vachtsevanos, Eds. New York, NY, USA: Springer, 2014.

[6] A. Abdulla, Z. Md Fadlullah, H. Nishiyama, N. Kato, F. Ono, and R. Miura, "Toward fair maximization of energy efficiency in multiple UAS-aided networks: A game-theoretic methodology," IEEE Trans. Wireless Commun., vol. 14, no. 1, pp. 305–316, Jan. 2015.

[7] L. Techy, C. Woolsey, and D. Schmale, "Path planning for efficient UAV coordination in aerobiological sampling missions," in Proc. IEEE Decision Control (CDC), 2008, pp. 2814–2819.

[8] J. Curry, J. Maslanik, G. Holland, and J. Pinto, "Applications of aerosondes in the arctic," Bull. Amer. Meteorol. Soc., vol. 85, no. 12, pp. 1855–1861, 2004.

[9] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: A survey," Comput. Netw., vol. 47, no. 4, pp. 445–487, 2005.

[10] B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, and A. Jamalipour, "A survey of routing attacks in mobile ad hoc networks," IEEE Wireless Commun., vol. 14, no. 5, pp. 85–91, Oct. 2007.

[11] Federal Aviation Administration, U.S. Department of Transportation.

(2015). New Rules for Small Unmanned Aircraft Systems [Online]. Available: http://www.faa.gov/news/press_releases/news_story.cfm? newsId=18295

[12] Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Standard 802.11, 2004.

Author Profile

N.Savitha working as Assistant Professor, Department of Computer Science in University College for Women, Koti, Hyderabad.