International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

Academic Science

Position Aware Secure Routing Approach for Airborne Mesh Network with Adaptive Channel Mechanism

Manjusha Anil Mane
Department Of E &TC Engineering,
Sinhgad College of Engineering, Pune,India.

Dr. AchalaDeshmukh
Associate Professor
Department Of E & TC Engineering,
Sinhgad College of Engineering, Pune,India.

Abstract-*In a Traditional way for wireless communication follows efficient routing by multi hop communication. Existing solutions still has many security concerns as WMNs can yields routing attacks. The network can be used mechanical way, and the attacker might manipulate data using black hole and worm hole attack, such as the IEEE 802.11i and the security mechanisms of the IEEE 802.11s mesh standard, are vulnerable to routing attacks as we experimentally showed in previous works. Proposed system present the position-aware, secure, and efficient mesh routing approach (PASER) in dynamic way to provide packet delivery with shortest path selection and provide more security to the data transmission on the network. This dynamic approach prevents more attacks than the IEEE 802.11s/i security mechanisms and the well-known, secure routing protocol ARAN, removes restrictive assumptions. Also prevent more networking attack on the network .Proposed system has similar performance like traditional PASER.*

Keywords-PASER, wireless network, Hop to Hop to communication, Key management, Channel aware routing.

I.INTRODUCTION

In a synopsis of the harms of the considerable east Japan seismic tremor and tidal wave in March 2011, that 1.9 million settled phone lines and 29,000 cell base stations were harmed. it uncovers that crisis rebuilding of correspondence systems took one month, while a full reclamation took 11 months. These certainties stress the expanding significance of versatile correspondence organizes in a fiasco regions. Also, these makes sense of point that a correspondence system that does not depend on existing framework and that can be sent in a considerably brief period (e.g., 60 minutes) is vital to effectively adapt to expansive scale emergencies. Independent Unmanned Aerial Vehicles (UAVs) going about as WLAN or LTE flying hotspots meet these necessities. In remote sensor organize bunching of sensor hubs is a standout amongst the most helpful techniques in view of its great adaptability and the support for information total. Information conglomeration consolidates information parcels from different sensor hubs into one information bundle by expelling same data.

a. Background

This lessens the transmission stack and the aggregate sum of information. With this vitality utilization is decreased in grouping, in light of the fact that the vitality load is all around adjusted by unique determination of bunch heads. By changing the bunch head part among other sensor hubs progressively in WSN, every hub is relied upon to use a similar measure of vitality after some time. In any case, as with common multi bounce sending, a CH around a sink has a tendency to have higher movement than different CHs. Therefore, hubs around sinks hub pass on sooner than different hubs, even in bunched WSN. In a numerous sink WSN, sensor hubs are isolated into a couple bunches. Sensor hubs inside a bunch are associated with one sink, which has a place with that group. Additionally, This paper proposed a Channel-aware Reputation System with adaptive detection threshold (CRS-A) to detect selective forwarding attacks in WSNs.

b. Motivation

Individual Unmanned Aerial Vehicles (UAVs) acting as WLAN or LTE aerial hotspots meet these requirements. Traditional PASER system are static In nature attacker can easily attack on the network using worm whole and black hole attacks proposed system act as dynamic in position which prevents physical

location access attack by the attacker. Clustering of sensor nodes in wireless sensor network is one of the most used method because of its good scalability and the support for data aggregation. These sensors are dividing into clusters and each then connecting to other and establish a network. Data aggregation combines data packets from multiple sensor nodes into one data packet by removing same information. This reduces the transmission load and the total amount of data. With this energy consumption is reduced in clustering, because the energy load is well balanced by dynamic selection of cluster heads. By changing the cluster head role among other sensor nodes dynamically in WSN, each node is expected to expend the same amount of energy over time. Previous techniques are less attack preventive .Using proposed system we can establish frequent and secure network using previous well establish security standards like ARAN and HWMP with our proposed scheme. proposed system provides Hop to Hop communication with efficient key management. Communication can takes place in hop to hop at the node to node it reduce traffic on the particular network pat. Mesh network reduces traffic overhead on the particular node .packets are traveled through the shortest path from source to destination. Hop to Hop communication manage through key pair identity of each node this provides strong authentication in the communication .this UAV's with its all equipment establish the quick network in seized area .

II. RELATED WORK

In [1] author proposed the security of WMNs, which is a key impediment to wide-scale deployment of WMNs, but thus far receives little attention. We first thoroughly identify the unique security requirements of WMNs for the first time in the literature. They propose ARSA, an attack-resilient security architecture for WMNs. In contrast to a conventional cellular-like solution, ARSA removes the need for establishing bilateral roaming agreements and having real-time interactions between potentially numerous WMN operators. With ARSA each user is no longer placed to any specific network operator, they must do in current cellular networks. Instead, he or she acquires a universal pass from a third-party broker whereby to realize seamless roaming across WMN domains administrated by different operators. Efficient mutual authentication and key agreement both between a user and a serving WMN domain and between users served by the same WMN domain supported by ARSA. In addition, ARSA is designed to be resilient to a wide range of attacks.

In[2] author proposed, state-of-the-art of security issues in MANET. In particular, they examine routing attacks, like link spoofing and colluding misrelay attacks, as well as countermeasures against such attacks in existing MANET protocols.

In [3] proposed coordinated flight of two autonomous UAVs to be used for aerobiological sampling of biological threat causes above agricultural fields. The periodic sampling task involves two phases: sampling interval and initialization interval. During the sampling interval, both vehicles must work their aerobiological sampling devices and follow an exact ground track in the presence of constant winds. During the interval, the vehicles move to their respective initial states to start the next sampling interval. Initialization interval must be as short as possible For maximization of the volume of air sampled by the UAVs during an individual sampling mission, they provided a simple, geometric method for generating candidate time optimal paths in steady winds, based on Dubins' well-known results for minimum time paths of bounded curvature. The approach is used to generate paths for both UAVs.

In[4] proposed PEACE, a novel Privacy-Enhanced yet Accountable security framework, tailored for WMNs. PEACE enforces strict user access control to manage with free riders and malicious users. On the other side, PEACE offers refined user privacy protection against both adversaries and various other network entities. PEACE is presented as a suite of authentication and key agreement protocols built upon our proposed short group signature variation. They shown that PEACE is resilient to a number of security and privacy related attacks.

In [5] author proposed IBC-HWMP, which was a secure Hybrid Wireless Mesh Protocol (HWMP) using identity-based cryptography(IBC). The reason for use IBC was that it does not need to verify the authenticity of public keys. They have implemented the IBC mechanism to secure control messages in HWMP, namely path request and path reply. They focus on secure data exchange in mutable fields.

In [6] author proposed they evaluated the original secure mesh route discovery protocol PASER, which had been designed to address the mesh network security in such critical environments. That protocol had been aimed to set up reliable ad-hoc routes between network nodes and to battle unauthorized nodes of working the route look-up process. Especially, its lightweight symmetric authentication scheme is noteworthy. The proposed protocol is investigated together with the previous well established routing protocols AODV, DYMO, BATMAN and OLSR under various scenario conditions and different attacks. At opposite of that, results show that PASER is able to secure the network without noticeable computational overhead. System reveals that PASER outpaces its matching part in many cases in terms of packet delivery ratio and maximum end-to-end delay.

In [7] author proposed Security in mobile ad-hoc networks (MANETs) continues to attract attention after years of research. Recently advancement in identity-based cryptography (IBC) sheds light on this problem and has become popular as a solution base. Scheme was presented for a comprehensive picture and capture the IBC security applications in MANETs based on a survey of publications on this topic since the emergence of IBC in 2001.

In [8] author proposes they formulates a locational optimization problem that achieves even deployment while takes account of energy consumption due to sensor movement, and then proposes two iterative algorithms. They used algorithm, named Lloyd-α, reduces the movement step sizes in Lloyd‘s method. It saves traveling distance while maintaining the convergence property. However, it leads to a larger number of deployment steps. The second algorithm, named DEED (Distributed Energy-Efficient self-Deployment), reduces sensor traveling distances and requires a comparable number of deployment steps as that in Lloyd‘s method. They also proposed an spontaneous method to deal with limited sensor communication range that is applicable to all three methods.

In [9] author proposed the IBE-RAOLSR and ECDSA-RAOLSR protocols for WMNs (Wireless Mesh Networks), which contributes to security routing protocols. They applied IBE (Identity Based Encryption) scheme and ECDSA scheme (Elliptic Curve Digital Signature Algorithm) methods to secure messages in RAOLSR (Radio Aware Optimized Link State Routing), namely TC (Topology Control) and Hello messages and compare ECDSA-based RAOLSR with IBE-based RAOLSR protocols.

In [10] author proposed fundamental research challenge such networks, which is how to fairly maximize the energy efficiency (throughput per energy) in networks comprising adaptive modulation-capable ground nodes. They demonstrate how adaptive modulation is affected For the mobility pattern intrinsic to the UASs.

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 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 around 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 APPROACH

Proposed system provides a security analysis as well as an extensive performance evaluation of PASER and three representative alternate solutions. ARAN: And secure routing protocol Authenticated Routing for Ad hoc Networks. HWMPS: A combination of thesecurity mechanisms of the IEEE 802.11s mesh standardand the Hybrid Wireless Mesh Protocol, whichis specified in the mentioned standard. BATMANS: Acombination of the IEEE 802.11i security mechanismsand the Better Approach to Mobile Ad hoc networkingproactive routing protocol, which iswidely deployed in community networks.

Adaptive channel aware packet routing techniques is used to energy efficient data transmission in the airborne mesh network. Since sensor nodes are deployed in open area and lackadequate physical protection, they may be compromised byadversaries through physical capture or software vulnerabilities

to misbehave in data forwarding. This paper consider data delivery ratio as the primary metric of network performance. Although, This system can detect the malicious nodes by CRS-A, it is unreasonable to isolate all the malicious nodes from the data forwarding path.

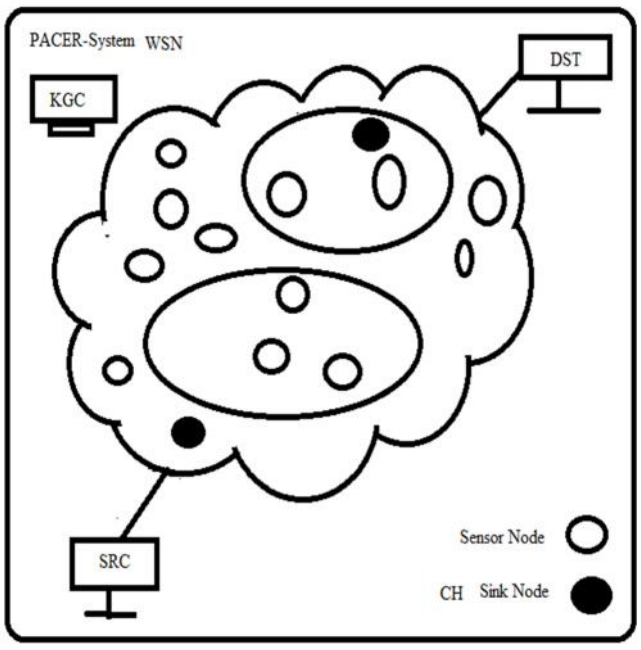

Fig.1. Proposed System Architecture

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

Academic Science

IV. MATHEMATICAL MODELING

Let **G= (V, E)** be a weighted graphwith weightFunction **w: E->R**mapping edges to real-valued weights.

If e= (u , v), we write w(u , v) for w(e)

The **length** of a path p= (v_0, v_1 , v_2,…v_k) is the sum of the weights of its constituent edges:

$$\text{length}(p) = \sum_{i=1}^{k} w(v_{i-1}, v_i).$$

The **distance** from u to v , denoted sigma (u ,v) , is the length of the minimum length path if there is a path from u to v and is infinity otherwise.

Adaptive Channel Aware Routing:-

Adaptive channel aware wireless sensor network is used to energy efficient packet transmission to overcome packet transmission delay in the network.

A. Destination Sequenced Distance Vector

Destination Sequence Distance Vector (DSDV) protocol is based on Bellman – Ford routing algorithm where each node maintains a routing table that contains the shortest path to every possible destination in the network and number of hops to the destination. The sequence n umbers allow the node to distinguish stale routes from new ones and avoid routing loops. A new broadcast route contains

- Destination Address

- Number of hops to reach the destination

-Sequence number of the information about the destination and a new sequence number unique to broadcast.

Updates in the routing tables are done periodically to maintain table consistency. The routing table consisting of Destination address

Graph: G = (N, E)

N = set of routers= {u, v, w, x, y, z}

E= set of links = {(u, v), (u, x), (v, x), (v, w), (x, w), (x, y), (w, y), (w, z)

Remark: Graph abstraction is useful in other network contexts

Example: P2P, where N is set of peers and E is set of TCP connections

B. Distance Vector Algorithm

This algorithm computed shortest distance by bell man ford solution to get minimum distance between nework.

$D_x(y)$ = Cost of least cost path from x to y. Then,

$D_x(y) = \min \{c (x, v) + D_v(y))$

Where, D is Shortest Distance of X and Y coordinate it. That is C, is cost for shortest path between tow vectors.

To investigate the impact of position deviation of assisting nodes, we introduce a new variable in our simulation - PER (position error ratio), which is defined asPER = distance from actual position to the ideal center / transmission range.

C. Cryptography

Cryptography is way to secure data transmission in the wireless airborne mesh network.The encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting cipher text is feasible

1. Encryption

Encrypts plain text m. cipher text

c = g^m * r^nmod n^2.

This function automatically generates random input r (to help with encryption).

2. Decryption

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand.

DecryptsCypher Text

c. Plain Text m = L(c^LAMBDAmod n^2) * u mod n,

Where, u = (L(g^LAMBDAmod n^2))^(-1) mod n

V. RESULT ANALYSIS

This work introduces the system model for deployment of sensor nodes in Wireless Sensor Network. Proposed system have analyzed the issue of energy hole problem and node placement problem in existing systems. Node deployment strategy has significant influence on limiting energy hole problem and optimizing network lifetime. Proposed system is devised a 3 Dimensional node deployment strategy by considering multi objective wireless. Using target localization to deploy sensor system selects nodes which is having minimum cost for data transmission. It formulates the problems of sensing and connectivity. Coverage is one of the most important performance metrics for sensor network reflects how well a sensor field is monitored. Our future work includes increase the capacity of sensor nodes by providing solar energy support to nodes which helps nodes active for long.

Energy efficient data transmission with secure dynamic source routing is measured by CRS-A to decrease delay towards packet transmission.

a. Simulation Parameter

Parameter	Value
Simulation Time	500 ms
Terrain Area	600 * 500
Time Arrival	32 ms
Protocol	PASER
No of Node	25, 45, 100

Table.1. Simulation Parameter

b. Comparison with similar System

Goals	Existing System%	Proposed System%
Throughput	70%	90%
Network	UAV-WMN	Wireless Mesh Network
Controller	KDC	Hop by Hop security
Security	Symmetric Key	Asymmetric Key
Protocol	IEEE 802.11i	PASER
Algorithm	AODV	DSR- Cluster wise +Adaptive Channel aware routing
Message Authentication	Keyed Hash messages	Additive Homomorphic Cryptography

Table.2. Comparison of System

c. Performance Measures

Proposed system aims to improve throughput maximization by reducing packet loss during wireless communication. Optimal sensor deployment helps to maximize network. Proposed system produces result to prove energy efficient wireless mesh network. Detect faulty node in wireless communication and

implementation for security norms. Wireless sensor network maximization of throughput by reducing packet delay ratio. We diagnose that PASER secure routing approach in UAV-WMN. It is shown that PASER reduces in the different case more attacks than the well-known, secure routing protocol ARAN and the standardized security mechanisms of IEEE 802.11s/i. 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 reasoned. We intend to investigate the use of PASER in a broader range of application scenarios.Proposed PASER is designed to implement wireless mesh network for packet transmission using security mechanism like Asymmetric key cryptography and message encoding scheme for authentication and authorization. Energy efficient is measure in the form adaptive channels selected for packet transmission.

Delay

This graph shows packet transmission delay for verification and channel aware packet transmission. End to end delay defined as the total time required reaching the packet from source to destination. Fig 2represents the results of End to End Delay of the system.

Average End to End Delay=1/Throughput

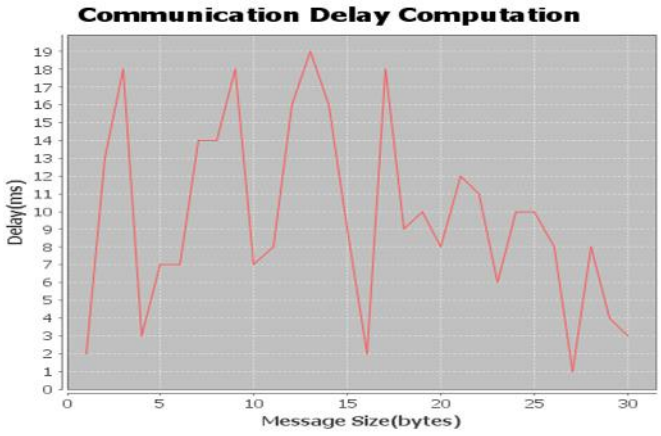

Fig. 2 Delay Computation

The end to end delay can be defined as the time utilized in taking the packet across the network. It is a one waydelay for the packet to be transmitted from source to destination.

Throughput

Throughput is defined as the rate of successful message delivery in a given time. Proposed system aims to improve throughput maximization by reducing packet loss during wireless communication. Wireless sensor network maximization of throughput by reducing packet delay ratio.

Throughput=Number of packet/Time taken

Fig.3 shows graph between number of packet count and time in milliseconds.

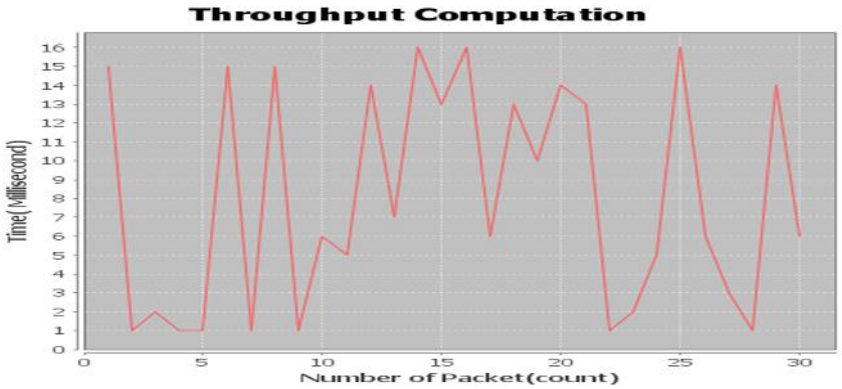

Fig. 3 Throughput Computation

International Journal of Electronics, Electrical and Computational System
IJEECS
ISSN 2348-117X
Volume 6, Issue 8
August 2017

Delivery Ratio

Packet delivery ratio is characterized as the ratio of total number of packets received by the destination node to the total number of packets transmitted by the source node.

Packet Delivery Ratio is characterized as the proportion of information packets got by the destinations to those dispatched by the sources.

PDR = Total no. of packets delivered / Total No. of packets dispatched.

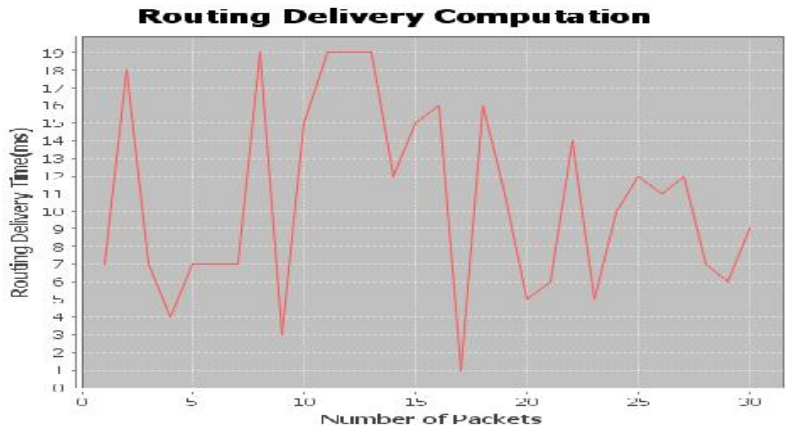

Fig. 4 Delivery Ratio Computation

Packet Loss Ratio

This graph shows that packet loss during data collection in WSN improved novel enrouting transmission with polynomial authentication and check polynomial reduces packet loss ratio.

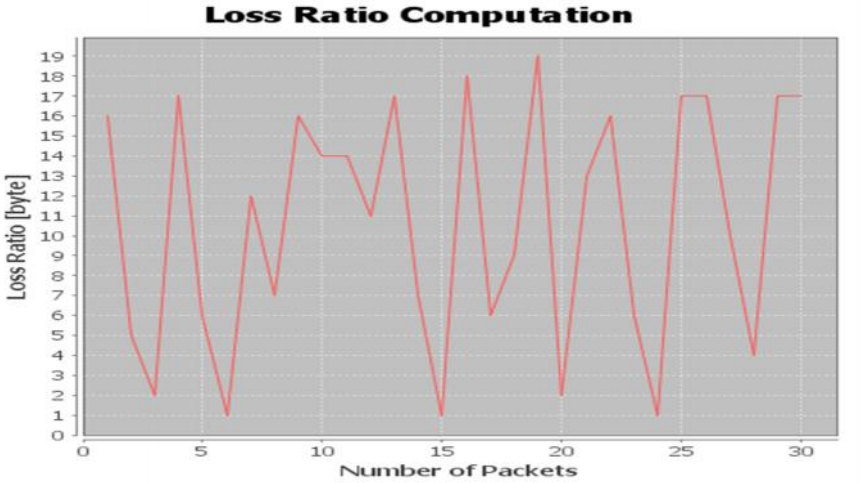

Fig. 5 Packet Loss Ratio

VI. CONCLUSION

We diagnose that PASER secure routing approach in UAV-WMN. It is shown that PASER reduces in the different case more attacks than the well-known, secure routing protocol ARAN and the standardized security mechanisms of IEEE 802.11s/i. 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 reasoned. This system intends to investigate the use of PASER in a broader range of application scenarios.

Academic Science

Proposed system implementation demonstrate with warm hole and black hole attack on sensor nodes by detecting and overcoming different attacks which are vulnerable to premature link failure in the network communication. Energy efficient and secure routing protocol is used for adaptive channel aware packet encryption with additive homomorphic packet transmission. This system emphasize on message or content encoding with 128 bit hash key by SHA256 algorithm. Wireless sensor node security can be achieved by node authentication with secret key of asymmetric key security along with Group Transient Key mechanism. Proposed wireless network build in unmanned mesh network with intermediate node communication.Proposed system implementation enhances airborne mesh network security with additive homomorphic cryptography for message encryption and decryption. Proposed work can be enhanced by real time implementation with airborne vehicle network to deal traffic management and cooperative communication to overcome collision in network traffics.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] N. Saxena and N. S. Chaudhari, "EasySMS: a convention for end-to-end secure transmission of SMS," IEEE Transactions on Information Forensics and Security, vol. 9, no. 7,Jul. 2014, pp.1157-1168.

[2] Tanya Brewer, Nelson Hasting, Scott Saunders, "Rules for keen matrix digital security: strong investigations and references," NISTIR 7628, The Smart Grid Interoperability Panel - Cyber Security Working Group,vol. 3 Aug.2010.

[3]H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Proficient verification and key administration components for savvy network correspondence," IEEE Systems Journal, vol. 8, Jun.2014, pp. 629-640.

[4] X. Huang, Y. Xiang, E. Bertino, J. Zhou, and L. Xu, "Powerful multi-calculate validation for delicate interchanges," IEEE Tr. on Dependable and Secure Comp., vol. 11, no. 6, Dec. 2014 pp. 568-581.

[5] D. Boneh and M. K. Franklin, "Personality based encryption from the weil blending," in Proc.CRYPTO,S.B.,USA,Aug.2001,pp. 213-229.

[6] Y. S. Kim and J. Heo, "Gadget verification convention for brilliant matrix frameworks utilizing homomorphic hash," Journal of Communications and Networks, vol. 14, no. 6, Dec. 2012,pp. 606-613.

[7] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Gadget verification component for brilliant vitality home zone systems," in Proc. IEEE ICCE, Las Vegas, USA, Jan. 2011, pp.787-788.

[8]ManimaranGovindaras, Adam Hann and Peter Sauer,"Cyber-physical frameworks security for Smartgrid",Feb.2012,p.29.wise.edu/records/distributions/papers/fgwhitepapers/govindarasu_future_grid_white_paper_cps_feb2012.pdf.

[9] NeteshSaxena, Bong Jun Choi, Rongxing Lu, "Verification and Authorization Scheme for different User Roles and Devices in SmartGrid", IEEE Transactions on Information Forensics and Security ,Volume:11 , Issue: 5 ,2016,pp. 907 – 921.

[10] H. Khurana and M. Hadley, "Shrewd network security issues," IEEE Security and Privacy Magazine, vol. 8, no. 1,Feb. 2010, pp. 81-85.

[11] H. Li, R. Lu, L. Zhou, B. Yang, and X. Shen, "An effective merkle-tree-based confirmation conspire for keen network," IEEE Systems Journal, vol. 8, no. 2, May. 2014, pp.655-662.

[12] H. Nicanfar, P. Jokar, K. Beznosov, and V. C. M. Leung, "Productive verification and key administration instruments for shrewd network correspondence," IEEE Systems Journal,vol. 8, no.2,Jun. 2014, pp. 629-640.

[13] R. Tabassum, K. Nahrstedt, E. Rogers, and K. S. Lui, "SCAPACH: versatile secret word changing convention for keen network gadget confirmation," in Proc.ICCCN, Nassau,Bahamas, Aug. 2013, pp. 1-5.