ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 4, Issue 12, December 2016

Position Aware Secure Routing Using Mesh Network in WNS

Ajit N Pawar

M.E, Dept. of Computer, RMD Sinhgad School of Engineering, Savitribai Phule University, Pune, Maharastra, 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 etc.

I. INTRODUCTION

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, theymust 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 anexact ground track in the presence of constant winds. During the interval, the vehicles move to their respective initial states to startthe 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 battleunauthorized nodes of working the route look-up process.Especially, its lightweight symmetric authentication scheme isnoteworthy. The proposedprotocol 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] authorproposed 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 comprehensivepicture 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. Furthermore, they formulated the problem of maximizing fair energy efficiency as a potential game that is played between the multiple ground nodes and substantiate its stability, optimality, and convergence. Based on the formulated possible scenario, a data collection method is proposed to maximize the energy efficiency with a fairness constraint.

III.GOALS AND OBJECTIVE

The high level control of the over UAV attack through the ground station and the direct control of each UAV using a safety pilot, which burdens pushing UAV-WMN to sensor deployment. Except that, because UAVs depend on the interchanging of information for cooperative node positioning, an attacker might change paths of the UAVs by selectively dropping packets. Problem is to avoid packet drop and prevent attacker to compromise network credential. as long as there is no efficient way to refresh those credentialsIn case the attacker is able to compromise the network credentials , the attacker might use data or even inject corrupted control information that could lead to the high jacking of a UAV. System provides active trust based routing scheme for secure communication in wireless sensor network. also providing the load balancing, reduseddelay, increasing life WNS.

IV. PROPOSED ALGORITHM

Encoding Algoritham :
Steps:
1. Representation of each letter in secret message by its equivalent ASCII code.
Conversion of ASCII code to equivalent 8 bit binary number.
2. Division of 8 bit binary number into two 4 bit parts. to the 4 bit parts.
3. Meaningful sentence construction by using letters obtained as the first letters of suitable words.
4. Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.
5. Encoding is not case sensitive.

Decoding
Steps:
1 First letter in each word of cover message is taken and represented by corresponding 4 bit number.
2 4 bit binary numbers of combined to obtain 8 bit number.
3 ASCII codes are obtained from 8 bit numbers.
4 finally secret message is recovered from ASCII codes

V. PROPOSED SYSTEM ARCHITECTURE

Proposed system provides a security analysis as well as an improved performanceevaluation of PASER and three representativealternate solutions. ARAN: And secure routing protocol Authenticated Routing forAd 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

VI.CONCLUSION

We diagnose that PASER secure routing approach inUAV-WMN. It is shown that PASER reduces in the different case more attacks than the well-known, securerouting protocol ARAN and the standardized security mechanismsof IEEE 802.11s/i. The efficiency of PASER is exploredin a theoretical and simulation-based analysis of its route discoveryprocess, and its scalability with respect to networksize and traffic load is reasoned. This system intend to investigate the use of PASER in a broader range ofapplication scenarios.

REFERENCES

1) Yanchao Zhang, Member, IEEE, and Yuguang Fang, Senior Member IEEE, "ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 10, OCTOBER 2006.
2) BOUNPADITH KANNHAVONG, HIDEHISA NAKAYAMA, YOSHIAKI NEMOTO, "A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS,"IEEE Wireless Communication ,October 2007 1536-1284/07/$20.00 © 2007 IEEE.
3) 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.
4) K. Ren, S. Yu,W. Lou, and Y. Zhang, "PEACE: A novel privacy-enhanced yet accountab security framework for metropolitan wireless mesh networks," IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 2, pp. 203–215,Feb. 2010.
5) 5)J. Ben-Othman and Y. Saavedra Benitez, "IBC-HWMP: A novel secure identity-based cryptography-based scheme for hybrid wireless mesh protocol for IEEE 802.11s," Concurr. Comput. Practice Exp., vol. 25, no. 5, pp. 686–700, 2013.
6) M. Sbeiti, J. Pojda, and C. Wietfeld, "Performance evaluation of PASER—An efficient secure route discovery approach for wireless mesh networks," in Proc. IEEE Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC), 2012, pp. 745–751.
7) S. Zhao, A. Aggarwal, R. Frost, and X. Bai, "A survey of applications of identity-based cryptography in mobile ad-hoc networks," IEEE Commun. Surveys Tuts., vol. 14, no. 2, pp. 380–400, May 2012.
8) Yuan Song, Bing Wang, Member, IEEE, Zhijie Shi, Member, IEEE, Krishna Pattipati, Fellow, IEEE,Shalabh Gupta, Member, IEEE, "Distributed Algorithms for Energy-efficientEven Self-deployment in Mobile SensorNetworks"IEEE TRANSACTIONS ON MOBILE COMPUTING
9) Y. Saavedra Benitez, J. Ben-Othman, and J. Claude, "Performance evaluation of security mechanisms in RAOLSR protocol for wireless mesh networks," in Proc. IEEE Int. Conf. Commun. (ICC), 2014, pp. 1808–1812.
10) A. Abdulla, Z. MdFadlullah, 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.WirelessCommun., vol. 14, no. 1, pp. 305–316, Jan. 2015."