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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

A Secure Scheme against Replication Attack for Heterogeneous Sensor Networks

Amruta Gaikwad, Prof. Rachana Satao

Dept. of Computer Engineering, Savitribai Phule Pune University, SKNCOE, Pune, India

ABSTRACT: Heterogeneous sensor networks (HSNs) comprise of few effective High-end sensors (H-sensors) and a substantial number of Low-end sensors (L-sensors). HSNs are susceptible against H-sensors replication attack. In this paper, a plan against the attack is proposed. The network analysis and simulationoutcomes demonstrate that the plan can enhance systems' strength against H-sensors replication attack as contrasted and existing related plans. The contribution work is, select distributed network use Pareto Optimal solution for multi-objective optimization problem. Limited local information using a user can select a new network device with high channel capacity and low blocking probability by using the proposed scheme.The experimental results show that the proposed scheme promotes the total throughput and reduce the probability of pairwise key establishment between replication H-sensors and normal L-sensors.

KEYWORDS: Heterogeneous Sensor networks, H-sensors replication attacks, master-slaver model, EQ method, multi-objective optimization

I. INTRODUCTION

Heterogeneous sensor networks (HSNs), which comprise of few H-sensors (e.g., PDAs) and a substantial number of L-sensors (e.g., the MICA2-DOT), have pulled in much consideration because of their better execution and adaptability contrasted and homogeneous sensor networks. In HSNs, H-sensors are accountable for sending data to the Base station (BS). Therefore, they are vulnerable to suffer from different types of attacks; one of the most common attacks is replication attack. This attack once being begun successfully, HSNs will be subject to the following threats: 1. L-sensors will choose these replication nodes as cluster heads and submit their data to them; 2. These replication nodes can communicate with normal H-sensors in the networks, and can forge a great deal of false data. This false data is forwarded to the BS, which not only wastes power and bandwidth of H-sensors, but also lets the BS make wrong judgments.

To improve the secrecy of HSNs, over the most recent couple of years, different pairwise key distribution schemes using symmetric key algorithms have been developed. In the AP-D scheme utilizes asymmetric predistribution key (AP) strategy, before deployment, an L-sensor and an H-sensor randomly select keys from a large key pool without replacement, respectively. After deployment, two nodes can establish a pairwise key if the number of common keys between them is greater than or equal to 1. In AP-L, the key pool of L-sensors is a subset of H-sensors. The CSS-SH scheme enhances the resilience by exploiting two dimensional backward key chains constructing disjoint and association key pools. All things considered, in the schemes, H-sensors and L-sensors share the same key pool; and H-sensors are needed to participate in the

establishment of shared keys between them. As a result, replication H-sensors can easily establish pairwise keys with normal nodes by using compromised keys. Therefore, in HSNs, new schemes against H-sensor replication attack must be developed.

In this paper, a secure scheme against H-sensors replication attack, namely SS-H, is proposed. Main contributions of our scheme are summarized as follows: 1. A new secure communication model, namely master-slaver model, is created, and is realized using new two-dimension backward key chains; 2. A new method, namely *EQ*, for establishing pairwise key between an L-sensor and an H-sensor is presented. 3. Solve the transformed maximization

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

problem in polynomial time and linear space. The solution of the transformed maximization problem is a Pareto Optimal result of the original multi-objective optimization problem.

II. EXISTING SECRET SCHEME AND HANDOVER SCHEME

I. Secret Scheme

The paper [1] presents a design methodology to build a hierarchical large-scale ad hoc network using different types of radio capabilities at different layers. In such a structure, nodes are first dynamically grouped into multi-hop clusters. Each group selects a cluster-head to be a backbone node (BN). Then higher-level links are established to connect the BNs into a backbone network. The LANMAR ad-hoc routing uses the notion of landmarks to keep track of such logical groups. In the LANMAR scheme, route the packet toward the corresponding remote landmark along a long multi-hop path. Advantages are: Selects shortest paths to remote nodes, small end-to-end delay, high quality link, enlarged network capacity, and QoS support etc. It provides reliable and fault tolerant system. In the paper [2],an effective key managementschemes – the asymmetric pre-distribution(AP) scheme for heterogeneous sensor networks.The powerful H-sensors are utilized to providesimple, efficient and effective key set up schemesfor L-sensors. The scheme utilizes strong capabilities of H-sensors in computation, communication, storage, energy supply and reliability. The AP scheme includes three phases: key pre-distribution phase, shared-key discovery phase, and H-sensor based pairwise key setup phase. Advantages are: It provides better security, with low complexity and significant reduction on storage requirement. Disadvantages are: Tamper-resistant hardware is too expensive. The distributed key management scheme [3] in distributed peer-to-peer wireless sensor networks with heterogeneous sensor nodes. There are three steps in the framework to establish pair-wise keys between the sensor nodes: (a) initialization, (b) direct key setup, and (c) (optional) path key setup. Analytical models are developed to evaluate the performance of the scheme in terms of connectivity, reliability and resilience. Advantages are: A wireless sensor network can achieve higher key connectivity and higher resilience. Increase the reliability of network.In static HSNs [4], a continuous secure scheme is proposed based on two-dimensional backward key chains. In the scheme, powerful sensors do not need to be equipped with tamper-resistant hardware.CSS-SH has three phases: key predistribution, shared key establishment, and path key establishment. In CSS-SH, after the shared key establishment phase, keys from the key pool saved in a node are hashed. Advantages are: To apply two dimensional backward key chains technique to HSNs, *n* disjoint and interrelated key pools are constructed. Increase the performance in continuous security, constructing disjoint and interrelated key pools is a simple and suitable method.In [5] paper, aiming at continuous secure in MDSNs, we propose a continuous secure scheme based on two-dimensional backward hash key chain technique. The security and performance analysis indicates that the proposed scheme achieves high local connectivity with a low storage overhead, and has higher network resilience against node compromise as compared with the schemes in for MDSNs.Advantages are: High local connectivity, low storage overhead and high network resilience.

II. Handover Scheme:

In the paper [6], study the handover measurement of a generic mobile cellular network with an arbitrary number of base stations. Design a unified framework for the network analysis and optimization. The exposition focuses on the stochastic modeling and addresses its key probabilistic events, namely: 1) suitable handover target found; 2) service failure; 3) handover measurement triggering; and 4) handover measurement withdrawal. Advantages are: to reduce terminal's battery consumption. In [7] paper, proposes a network selection strategy for vertical handoff. The Software-Defined Network (SDN) controller selects networks for mobiles in three phases: initialization, request matrix construction and network selection. The proposed scheme ensures that, a mobile will transfer to the most appropriate network at the most appropriate time. Advantages are: reduces the number of vertical handoffs, and maximizes the overall QoS significantly. An appropriate automatic network selection (ANS) mechanism [8], able to always select the best accessnetwork, is needed. This consists on constantly monitoring anytype of available access networks, automatically selecting andswitching to the best one, as the network that maximizes theusers' quality of experience taking into account their preferencesas well as the terminal and network conditions. ANS is a multi-dimension decision-making problem which can be solvedby finding an appropriate complex trade-off between possiblyconflicting criteria. In this paper, proposes an analytical modelto capture the preferences of end-users. Advantages are: Automatic selects the best wireless access network. In [9] paper, design a new, efficient, and multi-objective solution for handover

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

from the source eNB to target eNB/HeNB in emerging LTE systems.AnHeNB (femtocell) is assumed to be on the boundary between the source eNBs (macrocell) under consideration and its neighboring eNBs/HeNBs. Incoming and outgoing handovers can use the bandwidth of the HeNB, as long as the handover region is covered by the HeNB, and an available FDCH can be found in this HeNB. Advantages are: Reduces the blocking probabilities of both new and handover sessions. It provides shorter delays and better goodputs. Disadvantage is due to unnecessary handovers decrease the performance. In [10] paper has presented a new framework for downlink cellular network analysis. It is significantly more tractable than the traditional grid-based models, and appears to track (and lower bound) a real deployment about as accurately as the traditional grid model (which upper bounds). Advantages are: It provides simple and tractable predictions of the SINR distribution in a cellular network and accurate. The coverage and rate are easily modified to include frequency reuse. Base station cooperation affects coverage and rate.

In [11] paper, a two-step vertical handoff decision algorithm based on dynamic weight compensation is proposed. This algorithm adopts the filtering mechanism to reduce the system cost and improves the conventional algorithm by dynamic weight compensation and consistency adjustment. Advantages are: ensures the accuracy in network selectivity, improves the performance of consistency, maximizes the total distance of networks, and seeks fairness of load distribution over APs and BSs.The proposed system [12] model of a linear direct conversion transmits system (DCT) for the WCDMA system. This model consists of a number of subsystems or circuit blocks: Digital Signal Generator, Digital to Analog Converters (DAC) and Reconstruction Filters, Modulator, Preamplifier and Power Amplifier, as well as RF Front-end components. The WCDMA signal is created in three main steps: spreading, scrambling and pulse shaping. Advantages are: To optimize the overall system performance, system modeling is the essential tool to allocate system budgets with accurate analysis, and therefore, minimize design iterations and reduce the time to market. The major novelty of IEEE 802.11g [13] is support of four different physical layers that combine the provision of IEEE 802.11a data rates together with backward compatibility to the old IEEE 802.11 and IEEE 802.11b specifications. The new features of the IEEE 802.11g standard are: The provision of four different physical layers. The mandatory support of the short preamble type. The ERP network attribute. Newly defined protection mechanisms that deal with interoperability aspects.The CTS-to-self mechanism. Advantages are: theIEEE 802.11g standard will become the most widely acceptedone in high-data-rate WLAN. The CTS-to-self mechanism is more efficient in clear channel conditions. But less robust than the RTS/CTS mechanism against hidden terminals. In [14] paper, concentrate on the user network selection decision for non-real-time data applications, which accounts for a large number of the new data services being developed. The user-centric strategy proposed in this paper is based on a maximizing the user's predicted consumer surplus while minimizing the data delays.[15] Paper proposes a novel fuzzy-logic (FL)-based decision-making algorithm for VHO, which is capable of combining the merits of both schemes to achieve excellent handover in terms of packet transfer delay for all the cases considered here. The strength of FL in handling uncertain and conflicting decision metrics is exploited. Advantages are decrease in packet transfer delay, and hence, a better QoS can be obtainedby performing proper VHO between the two media. In [16] paper, Wireless Multimedia Sensor Network supporting wide variety of the applications in the modern era motivates researchers to investigate various routing techniques. This paper investigates the state of art of research on routing techniques in WMSN and effect of mobility on these routing issues. Routing is a key factor which allows us to improve system performance in terms of various parameters like packet loss, delay and energy saving. We pointed out how recent work is implemented and incorporating dynamic plans and mobility factor in current work can enhance the capability of the WMSN [17]. Advantages are: The bandwidth utilization should be efficiently managed by multipath routing or by multichannel communication. The system is reliable means the ability to deliver data to the destination with minimum packet loss. The network can reduce the network failure and coverage problem effectively.

In heterogeneous sensor networks, H-sensors are accountable for sending data to the Base station (BS). Therefore, they are vulnerable to suffer from various attacks; one of the most common attacks is replication attack. This attack once being launched successfully, HSNs will be subject to the following threats: 1. L-sensors will choose these replication nodes as cluster heads and submit their data to them; 2. These replication nodes can communicate with normal H-sensors in the networks, and can forge a great deal of false data. This false data is forwarded to the BS, which not only wastes power and bandwidth of H-sensors, but also lets the BS make wrong judgments. Thus by studying the existing two schemes in detail we came to the conclusion of analysis that the following factors are remained unnoticed by many researchers.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

- HSNs are vulnerable to H-sensors replication attack.
- In AP-D, AP-L and CSS-SH, H-sensors and L-sensors share the same key pool. Further, an adversary can easily successfully launch replication H-sensors attack by capturing L-sensors.
- Doesn't guarantee that high energy/resources nodes always be chosen as cluster-head
- Doesn't control the number and even placement of cluster-heads
- Sensor nodes are energy critical.

In this paper, a secure scheme against H-sensors replication attack, namely SS-H, is proposed. Main contributions of our scheme are summarized as follows: 1. A new secure communication model, namely master-slaver model, is created, and is realized using new two-dimension backward key chains; 2. A new method, namely *EQ*, for establishing pairwise key between an L-sensor and an H-sensor is presented. We will also achieve the following objectives in the proposed system.

Objectives:

- To reduce the computational overhead and network traffic.
- To improve resiliency of H-sensor replication attack.
- Network selection should be to select a high performance network device and avoid being blocked.
- To select the network, maximizes the channel capacity and minimizes the blocking probability.
- Confidential multiuser communication with multi hops wireless communication.

III. PROPOSED SYSTEM

I. System Scenario:

In this paper, a secure scheme against H-sensors replication attack, namely SS-H, is proposed. Main contributions of our scheme are summarized as follows: 1. A new secure communication model, namely master-slaver model, is created, and is realized using new two-dimension backward key chains; 2. A new method, namely *EQ*, for establishing pairwise key between an L-sensor and an H-sensor is presented.

In HSNs, H-sensors serve as cluster heads and form clusters around them [3]. The formation of clusters is as follows: Each L-sensor selects an H-sensor whose Hello message has the best signal strength as its cluster head, and records other H-sensors from which it has received Hello messages, will serve as backup cluster heads in the case that the cluster head fails.

In SS-H, we make use of the following assumptions:

1. Only a limited number of L-sensors may be compromised by an attacker during the short time period of the key establishment between L-sensors.
2. BS and H-sensors will not be compromised by an attacker.

The Fig.1 shows the system architecture of heterogeneous wireless network which consists of Base Stations, clusters, cluster heads as H-sensors and L-sensors how to communicate each other.

Master-Slaver model

In this model, an H-sensor can calculate the key shared with an L-sensor, but an L-sensor cannot.

Key pool: The key pool, consists of two-dimensional backward hash key chains, is divided into two parts. One is key pool of H-sensors, and the other is key pool of L-sensors which consists of two parts: a second-dimensional generation key pool and an ordinary key pool.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

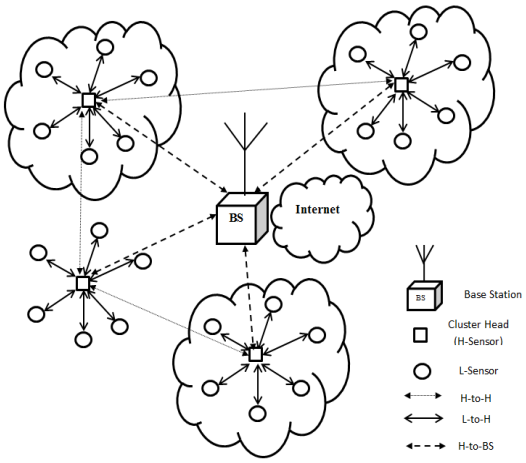

Fig.1 Proposed System Architecture

Our contribution of this paper is, to create Distributed Network Selection Scheme (DNSS) for heterogeneous wireless network. In DNSS, users are divided into two classes: non-handoff and handoff users. In our scheme, a handoff user is unable to find a network device which exactly provides maximal channel capacity and minimal blocking probability simultaneously either. By solving the maximization problem, a handoff user can select a new network device. We will prove that this selected new network device is a Pareto Optimal solution of the original multi-objective optimization problem.

Advantages of Proposed System:

1. Only a limited number of L-sensors may be compromised by an attacker during the short time period of the key establishment between L-sensors.
2. BS and H-sensors will not be compromised by an attacker.
3. EQ method is used to improve resiliency of H-sensor replication attack.
4. A user can select a new network device with high channel capacity and low blocking probability.
5. Computation and memory complexity is small.

II. Mathematical Module

Let us consider S as a set Secure Scheme for Wireless Sensor Networkswith wireless sensor node confidentiality

S= { }

INPUT:

- Identify the inputs as number of nodes

  F= {f_1, f_2, f_3 ……,f_n| 'F' as set of functions to execute to routing model}

  I= {i_1, i_2, i_3…|'I' sets of inputs to number of nodes/ sensors}

  O= {o_1, o_2, o_3….|'O' Set of outputs from the function sets}

  S= {I, F, O}

  I = {Number of nodes}

  O = {Shortest routing path for multi hop protocol}

  F = {AODV, ARQ, Euclidean distance, Pair wise key}

- **Two-dimensional backward key chain:**

The method for constructing a two-dimensional backward key chain $C_j$is as follows:

1. A backward key chain, whose length is *n*, is generated by a generation key $g_j$as follows:

$$k_j^i = H_1\left(k_j^{i+1}\right) Where, k_j^n = H_1\left(g_j\right),\ 1 \le i \le n-1 \qquad (1)$$

2. A forward key chain, whose length is *L*, is generated by a generation keyk_j^i as follows:

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

$k_j^{(i,l)} = H_2\left(k_j^i, k_j^{(i,l-1)}\right)\ Where, k_j^{i,l} = H_2\left(k_j^i, k_j^i\right),\ 1 \le l \le L$ (2)

1. Dijkstra's algorithm:

Dijkstra's algorithm on a graph with edges E and vertices V can be expressed as a function of the number of edges, denoted |E|, and the number of vertices, denoted |V|, using big-O notation. How tight a bound is possible depends on the way the vertex set Q is implemented. In the following, upper bounds can be simplified because $|E|=O(|V|^2)$for any graph, but that simplification disregards the fact that in some problems, other upper bounds on |E| may hold. For any implementation of the vertex set Q, the running time is in

$O(|E|.T_{dk}+|V|.T_{em})$ (3)

Where T_{dk} and T_{em} are the complexities of the *decrease-key* and *extract-minimum* operations in Q. The simplest implementation of Dijkstra's algorithm stores the vertex set Q as an ordinary linked list or array, and extract-minimum is simply a linear search through all vertices in Q. In this case, the running time is

$O(|E|+|v|^2)=O(|V|^2)$ (4)

FunctionDijkstra(*Graph*, *source*):
Create vertex set Q
For each vertex *v* in *Graph*: *// Initialization*
dist[*v*] ← INFINITY *// Unknown distance from source to v*
prev[*v*] ← UNDEFINED *// Previous node in optimal path from source*
add *v* to *Q// All nodes initially in Q (unvisited nodes)*
dist[*source*] ← 0 *// Distance from source to source*
While*Q* is not empty:
u ← vertex in *Q* with min dist[u] *// Select source node first*
remove *u* from *Q*
for each neighbor *v* of *u*: *// where v is still in Q.*
alt ← dist[*u*] + length(*u*, *v*)
if*alt*<dist[*v*]: *// A shorter path to v found*
dist[*v*] ← *alt*
prev[*v*] ← *u*
Returndist[], prev[]

2. Distributed Network Selection Scheme for Handoff User Algorithm:

Input: available network device set at time t $A_j(t)$, number of channels l_j , bandwidth per channel b_j, number of handoff and non-handoff users $\Gamma_{ji}(t)$ and $\Gamma \ominus_{ji}(t)$, received signal power $s_{jij}(t)$, noise interference power $\eta_{jij}(t)$ and basic bandwidth requirement γ_{jij}.

Output: network selection result $F_j(t)$.

Process:

Step 1: max=0, index=0;
Step 2: **for**$\forall a_{ji} \epsilon A_j(t)$**do**
Step 3: Calculate the channel capacity $q_{jij}(t)$.
Step 4: Estimate the blocking probability $p_{jij}(t)$
Step 5: **if**$q_{jij}(t) \ge \gamma_{jij}$**then**
Step 6: Calculate the throughput $\tau_{jij}(t)$
Step 7: **if** $\tau_{jij}(t) \ge max$**then**
Step 8: $\tau_{jij}(t) \to max$**then**
Step 9: the index of the selected network device *index* = *i*;
Step 10: **for** i=1;i≤ $|A_j(t)|$; i++ **do**
Step 11: **if** i==index **then**
Step 12:the selected network device is $a_{ji}, f_{jij}(t) = 1$;

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

Step 13: **else**
Step 14:$f_{jij}(t) = 0$;
Step 15: **return** $F_j(t)$;

IV. DESIGN AND DISCUSSION

Use case Diagram:

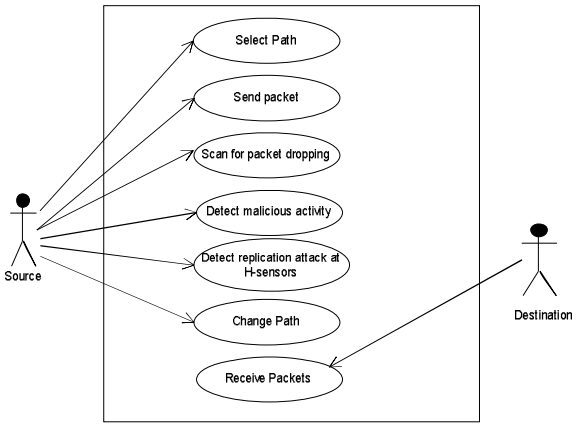

Fig.2. Use Case Diagram

A heterogeneous wireless sensor network has less High-end sensors and maximum Low-end sensors. First create the heterogeneous wireless sensor network using simulator. Give source address and destination address and transfer message. Key generation when two sensors communicate like L-sensors to H-sensors, H-sensors to H-sensors and H-sensors to Base station in source address to the destination address. Select the shortest path between source nodes to destination node. The message is divided into number of packets. Calculate the channel capacity from source to destination. Monitor neighboring nodes on selected path for detecting malicious attacks in network. If attack detects then change the path from source to destination. After receives the packet at destination. In this way, calculate the channel capacity, energy, throughput, packet delivery ratio, packet loss ratio, packet delay ratio and overhead etc.

V. CONCLUSION AND FUTURE WORK

In this paper, master-slaver model is applied in distributed network, is created, and is acknowledged using a new two-dimension backward key chain. In addition, *EQ* strategy is introduced. Analysis and simulation demonstrate that the master-slaver model can prevent replication H-sensors from communicating with normal H-sensors no matter how many L-sensors are compromised and the *EQ* strategy can fundamentally decrease the probability of pairwise key establishment between replication H-sensors and ordinary L-sensors. Based on constrained local information, a handoff user can select a new network device with high channel capacity and low blocking probability by using the proposed scheme. Moreover, the computation and memory complexities of the proposed scheme are relatively small. The future work comprised of implementing the system with heterogeneous wireless network with high-end and low-end sensors energy. The system can also be implemented in secure data transformation.

REFERENCES

[1] K. Xu, X. Hong, M. Gerla, "An ad hoc network with mobile backbones," in: ICC 2002, New York, NY, April 2002.
[2] X. Du, Y. Xiao, M. Guizani, et al., "An effective key management scheme for heterogeneous sensor networks," ad hoc networks, vol. 5, no. 1, pp. 24-34, 2007.
[3] K. Lu, Y. Qian, M. Guizani, et al, "A Framework for a Distributed Key Management Scheme in Heterogeneous Wireless Sensor Networks," IEEE Trans. on Wireless Communications, vol. 7, no. 2, pp. 639-647, 2008.

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

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 5, Issue 12, December 2017

[4] B. Zhou, J. Wang, S. Li, et al., "A Continuous Secure Scheme in Static Heterogeneous Sensor Networks", IEEE Communicatons Letters, vol. 17, no. 9, pp. 1868-1871, 2013.
[5] S. Li, B. Zhou, J. Dai, et al. "A secure scheme of continuity based on two-dimensional backward hash key chains for sensor networks," IEEE Wireless Communications Letters, vol. 1, no. 5, pp. 416-419, 2012.
[6] V. M. Nguyen, C. S. Chen, and L. Thomas. A unified stochastic model of handover measurement in mobile networks. Networking, IEEE/ACM Transactions on, 22(5):1559–1576, 2014.
[7] A software-defined network based vertical handoff scheme for heterogeneous wireless networks. In Global Communications Conference (GLOBECOM), 2014 IEEE, pages 4671– 4676. IEEE, 2014.
[8] Q. T. Nguyen-Vuong and et al. Multi-criteria optimization of access selection to improve the quality of experience in heterogeneous wireless access networks. IEEE transactions on vehicular technology, 62(EPFLARTICLE-182868):1785–1800, 2013.
[9] Abhishek Roy, Jitae Shin, and NavratiSaxena. Multi-objective handover in lte macro/femto-cell networks. Communications and Networks, Journal of, 14(5):578–587, 2012.
[10] J. G. Andrews, F. Baccelli, and R. K. Ganti. A tractable approach to coverage and rate in cellular networks. Communications, IEEE Transactions on, 59(11):3122–3134, 2011.
[11] C. Liu and et al. A two-step vertical handoff decision algorithm based on dynamic weight compensation. In Communications Workshops (ICC), 2013 IEEE International Conference on, pages 1031–1035. IEEE, 2013.
[12] C. W. Liu. Modeling 3g/wcdma/hsdpa handset transmit system. Microwave Product Digest, 2007.
[13] D. Vassis and et al. The ieee 802.11 g standard for high data rate wlans. Network, IEEE, 19(3):21–26, 2005.
[14] O. Ormond, P. Perry, and J. Murphy. Network selection decision in wireless heterogeneous networks. In Personal, Indoor and Mobile Radio Communications, 2005. PIMRC 2005. IEEE 16th International Symposium on, volume 4, pages 2680–2684. IEEE, 2005.
[15] J. Hou and D. O'brien. Vertical handover-decision-making algorithm using fuzzy logic for the integrated radio-and-ow system. Wireless Communications, IEEE Transactions on, 5(1):176–185, 2006.
[16] Borawake-Satao R, Prasad R. Comprehensive survey on effect of mobility over routing issues in wireless multimedia sensor networks. International Journal of Pervasive Computing and Communications. 2016 Nov 7; 12(4):447-65.
[17] Borawake-Satao R, Prasad R. Mobility Aware Path Discovery for Efficient Routing in Wireless Multimedia Sensor Network. In Proceedings of the International Conference on Data Engineering and Communication Technology 2017 (pp. 673-681). Springer Singapore.