iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 Issue: III Month of publication: March 2017

DOI: http://doi.org/10.22214/ijraset.2017.3042

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Copy Cat: Effective Identification and Removal of Copy Cat Nodes in WSN

B Vignesh[1], B A Shanmugavel[2], K Chandrasekar[3], K Sathyamoorthy[4], Dr.V. Subedha[5]
[1,2,3]*Student Fourth Year,* [4]*professor,* [5]*professor and Head*
[1,2,3,4] *Department Of CSE, Panimalar Institute Of Technology, Chennai-600123.*

Abstract: In this system, wireless sensor networks are more vulnerable to the node clone, and several distributed protocols have been proposed to detect this attack. So they require too strong assumptions that are to be practical for large-scale, randomly deployed sensor networks. In the proposed system, using distributed clone detection protocol namely ercd (energy-efficient ring based clone detection) protocol which has two stages: witness selection and legitimacy verification for clone detection. In the modification process, the first one is based on a distributed hash table (dht) in which the chord algorithm which is used to detect the cloned node, every node is assigned with the random key, before it transmits the data it has to give its key which would be verified by the witness node. If the same key is been given by another node then the witness node identifies the cloned node. Here every node only needs to know the neighbor-list containing all neighbor ids and its locations. We are implementing chord algorithm, by location based nodes identification, where every region/location will have a group leader. The group leader will generate a random number with the time stamp to the available nodes that are in that location. Witness nodes verify the random number and time stamp to detect the cloned node. The message is also encrypted for security purpose.

Index terms: witness node, wireless sensor networks (wsns), distributed hash table(dht).

I. INTRODUCTION

Wireless sensors have been widely deployed for variety of applications, that ranging from environment monitoring to telemedicine and objects tracking, etc. For cost-effective sensor placement, sensors are usually that are not tamper-proof devices and are deployed in places without monitoring and protection, which makes them prone to different attacks. For example, a malicious the user may get compromises some sensors and acquires their private information. Then, it can duplicate the sensors and deploy clones in a wireless sensor network (WSN) to launch a variety of attacks, which is been referred to as the clone attack. As the duplicated sensors have the same information, e.g., code and cryptographic information, captured from legitimate sensors, they can easily participate in the network operations and launch attacks. Due to the low cost for sensor duplication and deployment, clone attacks have become one of the most critical security issues in WSNs. Thus, it is been essential to effectively detect clone attacks in order to ensure healthy operation of WSNs. To allow efficient clone detection, usually, a set of nodes are selected, which are called witnesses, to help and certify the legitimacy of the nodes in the network. The private information of the source node, i.e., identity and the location information is shared with witnesses at the stages of the witness selection. When any of the nodes in the network wants to transmit data, it first sends the request to the witnesses for legitimacy verification, and witnesses will report a detected attack if that the node fails the certification. To achieve successful clone detection, witness selection and legitimacy verification should fulfill two requirements: 1) witnesses node that should be randomly selected; and 2) at least one of the witnesses can be successfully receiving all the verification message(s) for clone detection. The first requirement is to make it difficult for the malicious users eavesdrop the communication between current source node and its witnesses, so that malicious users cannot generate duplicate verification messages. The second requirement is to make sure that at least one of the witnesses node that can check the identity of the sensor nodes to determine whether there is a clone attack or not.

II. SYSTEM ANALYSIS

In the existing system, the Wireless sensor networks are vulnerable to the node clone, and several distributed protocols have been proposed to detect this attack. So they require too strong assumptions that are to be practical for large-scale, randomly deployed sensor networks. In the PROPOSED SYSTEM, using distributed clone detection protocol namely ERCD (Energy-Efficient Ring Based clone Detection) protocol which has two stages: witness selection and legitimacy verification for clone detection. In the MODIFICATION Process, The first one is based on the distributed hash table (DHT) in which Chord algorithm is been used to detect the cloned node, every node is assigned with the random key, before it transmits the data it has to give its key which would be verified by the witness node. If the same key is being given by another Node then the witness node identifies the cloned Node. Here every node only needs to know the neighbor-list containing all neighbor IDs and its locations. We are implementing Chord Algorithm, by location based nodes identification, where every region/location will have a group leader. The Group leader will generate a random number with the time stamp to the available nodes in that location. Witness nodes verify the random number and time stamp to detect the cloned node. The message is also encrypted for security purpose.

III. LITERATURE SURVEY

The Green, Reliability, and Security of Emerging Machine to Machine Communications
Rongxing Lu, Xu Li, Xiaohui Liang, and Xuemin (Sherman) Shen, Xiaodong Lin-April 2011
The gadget-to-device communications is characterized via regarding a big wide variety of intelligent machines sharing records and making collaborative decisions without direct human intervention. Because of its capacity to aid a big range of ubiquitous characteristics and attaining better cost performance, M2M communications has speedy grow to be a market-changing pressure for a extensive variety of actual-time monitoring applications, consisting of far off e-healthcare, clever homes, environmental tracking, and industrial automation. However, the flourishing of M2M communications nevertheless hinges on fully know-how and handling the existing challenges: electricity performance (inexperienced), reliability, and safety (GRS). Without assured GRS, M2M communications cannot be widely everyday as a promising conversation paradigm. In this article, we explore the emerging M2M communications in phrases of the potential GRS issues, and goal to promote an electricity-efficient, reliable, and comfy M2M communications environment. Particularly, we first formalize M2M communications structure to include three domain names — the M2M, community, and alertness domains — and for that reason outline GRS necessities in a systematic way. We then introduce some of GRS enabling techniques by way of exploring pastime scheduling, redundancy utilization, and cooperative security mechanisms. Those techniques maintain promise in propelling the development and deployment of M2M communications programs.

Wireless sensor networks: a survey
Y. Sankarasubramaniam, E. Cayirci-March 2002
This paper describes the concept of sensor networks which has been made possible by using the convergence of micro electro-mechanical structures generation, wireless communications and virtual electronics. First, the sensing tasks and the potential sensor networks packages are explored, and a evaluation of things influencing the design of sensor networks is provided. Then, the communiqué architecture for sensor networks is printed, and the algorithms and protocols developed for each layer within the literature are explored. Open studies troubles for the realization of sensor networks also are mentioned. 2002 published by means of Elsevier technological know-how B.V.

Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks
Anfeng Liu, Ju Ren, Xu Li, Zhigang Chen, Xuemin (Sherman) Shen-May 2012
The cost function primarily based routing has been broadly studied in wireless sensor networks for electricity performance improvement and network lifetime elongation. However, due to the complexity of the hassle, existing solutions have diverse obstacles. In this paper, we analyze the inherent elements, design principles and evaluation methods for value function based totally routing algorithms. Strength aware fee primarily based routing algorithms named Exponential and Sine fee function primarily based path (ESCFR) and Double value characteristic based path (DCFR) were proposed in this paper. For ESCFR, its price feature can map small modifications in nodal final energy to big modifications in the characteristic price. For DCFR, its cost function takes into consideration the stop-to-give up energy intake, nodal last electricity, resulting in a extra balanced and efficient strength utilization among nodes. The performance of the value characteristic layout is analyzed. Sizeable simulations show the proposed algorithms have considerably higher overall performance than present competing algorithms.

Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes
Tao Shu, Sisi Liu, and Marwan Krunz-July 2010
The Compromised-node and denial-of-provider are two key attacks in wireless sensor networks (WSNs). On this paper, we study routing mechanisms that avert (bypass) black holes formed by those assaults. We argue that existing multi-direction routing methods are susceptible to such assaults, mainly because of their deterministic nature. So as soon as an adversary acquires the routing set of rules, it could compute the equal routes recognized to the source, and therefore endanger all records sent over those

routes. On this paper, we broaden mechanisms that generate randomized multipath routes. Below our design, the routes taken by the "stocks" of different packets change over the years. So although the routing algorithm turns into recognized to the adversary, the adversary nevertheless can't pinpoint the routes traversed with the aid of every packet. Except randomness, the routes generated by way of our mechanisms are also extraordinarily dispersive and electricity-green, making them pretty able to bypassing black holes at low energy price. Tremendous simulations are performed to confirm the validity of our mechanisms.

A randomized countermeasure against parasitic adversaries in wireless sensor networks
P. Papadimitratos, J. Luo, and J. P. Hubaux-September 2010
Due to their restrained abilities, wireless sensor nodes are challenge to bodily attacks which might be hard to defend towards. On this paper, we first perceive a regular attacker, referred to as parasitic adversary, who seeks to exploit sensor networks by using obtaining measurements in an unauthorized manner. As a countermeasure, we first employ a randomized key refreshing: with low communication cost, it targets at confining (however not getting rid of) the effects of the adversary. Moreover, our low-complexity solution, GossiCrypt, leverages at the massive scale of sensor networks to protect information confidentiality, efficaciously and efficiently. GossiCrypt applies symmetric key encryption to facts at their supply nodes; and it applies re-encryption at a randomly selected subset of nodes en course to the sink. The mixture of randomized key clean and GossiCrypt protects data confidentiality with a opportunity of almost 1; we show this analytically and with simulations. Similarly, the electricity intake of GossiCrypt is lower than a public-key based solution by several orders of value.

Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs
Rongxing Lu, Xiaodong Lin, Tom H. Luan, Xiaohui Liang, Xuemin (Sherman) Shen-Janauary 2012
As a high target of the quality of privacy in vehicular ad hoc networks (VANETs), vicinity privacy is imperative for VANETs to completely flourish. Even though frequent pseudonym converting provides a promising solution for vicinity privateers in VANETs, if the pseudonyms are changed in a fallacious time or location, one of these answers may emerge as invalid. To deal with the issue, in this paper, we gift a powerful pseudonym converting at social spots (desktops) strategy to reap the provable place privacy. Particularly, we first introduce the social spots wherein numerous automobiles can also acquire, e.g., a avenue intersection while the site visitors light turns purple or a unfastened automobile parking space close to a shopping center. By means of taking the anonymity set length as the vicinity privacy metric, we then increase anonymity set analytic fashions to quantitatively inspect the region privations this is performed by means of the pcs approach. Further, we use sport-theoretic strategies to prove the feasibility of the computers strategy in exercise. Great performance opinions are performed to illustrate that higher region privacy may be executed while a automobile adjustments its pseudonyms at some pretty social spots and that the proposed desktops approach can assist motors to intelligently trade their pseudonyms at the right moment and location.

An Early Warning System Against Malicious Activities for Smart Grid Communications
Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki-May 2011
The smart grid (SG) provides the most important increase capacity within the gadget-to-system (M2M) market these days. Spurred by using the latest advances in the M2M technologies, the clever meters/sensors used in smart grid are predicted no longer to require human intervention in characterizing power necessities and power distribution. These numerous sensors are able to file again the facts including energy intake and other monitoring indicators. However, SG, because it incorporates an strength control and distribution machine, requires fast response to malicious activities along with allotted Denial of provider (DDOS) assaults towards clever meters. In this newsletter, we model the malicious and/or bizarre activities, which may also compromise the security and privations of smart grid customers, as a Gaussian process. Based totally on this model, a singular early warning gadget is proposed for awaiting malicious events within the SG network. With the caution device, SG manage middle can forecast such malicious activities, thereby allowing SG to react beforehand and mitigate the possible effect of the malicious interest. We confirm the effectiveness of the proposed early caution device via computer-primarily based simulations.

A Dynamic Privacy-Preserving Key Management Scheme for Location Based Services in VANETs
Rongxing Lu, Xiaodong Lin, Xiaohui Liang, Xuemin(Sherman) Shen-Janauary 2012
In this paper, to obtain a car user's privations protection even as improving the important thing update efficiency of region-primarily based offerings (LBSs) in vehicular ad hoc networks (VANETs), we endorse a dynamic privacy-maintaining key control scheme called DIKE. Specially, within the proposed DIKE scheme, we first introduce a privacy-preserving authentication method that not

simplest affords the automobile consumer's anonymous authentication but permits double-registration detection as well. We then gift efficient LBS session key update strategies: 1) We divide the session of an LBS into numerous time slots in order that on every occasion slot holds a different session key; whilst no automobile person departs from the provider consultation, every joined consumer can use a one-manner hash feature to autonomously update the brand new session key for achieving forward secrecy. 2) We additionally combine a unique dynamic threshold technique in conventional vehicle-to-vehicle (V-2-V) and automobile-to-infrastructure (V-2-I) communications to obtain the session key is backward secrecy, i.e., while a car person departs from the service consultation, extra than a threshold number of joined users can cooperatively update the new session key. Performance evaluations via significant simulations exhibit the efficiency and effectiveness of the proposed DIKE scheme in phrases of low key replace put off and fast key update ratio.

Distributed Detection of Clone Attacks in Wireless Sensor Networks
Mauro Conti,Roberto DiPietro,Luigi Mancini-October 2011
The Wi-Fi Sensor Networks (WSNs) are often deployed in hostile environments wherein an adversary can physically seize some of the nodes, first can reprogram, and then, can replicate them in a large variety of clones, easily taking control over the community. A few dispensed solutions to deal with this fundamental problem had been recently proposed. However, these answers are not exceptional. First, they may be energy and reminiscence annoying: A serious downside for any protocol to be used in the WSN-resource-limited surroundings. Further, they're susceptible to the specific adversary models introduced on this paper. The contributions of these paintings are threefold. First, we examine the ideal residences of a dispensed mechanism for the detection of node replication assaults. 2nd, we show that the recognized answers for this trouble do no longer completely meet our requirements. 0.33, we suggest a brand new self-recovery, randomized, green, and disbursed (red) protocol for the detection of node replication attacks, and we show that it satisfies the added requirements. In the end, enormous simulations show that our protocol is tremendously green in communiqué, reminiscence, and computation; is much greater powerful than competing solutions inside the literature; and is proof against the new type of attacks brought in this paper, whilst different answers aren't.

Distributed Detection of Node Replication Attacks in Sensor Networks
B. Parno, A. Perrig, and V. Gligor-May 2005
The low-cost, off-the-shelf hardware additives in unshielded sensor-network nodes depart them prone to compromise. With little effort, an adversary can also capture nodes, examine and mirror them, and surreptitiously insert these replicas at strategic locations in the community. Such assaults may have extreme effects; they will allow the adversary to corrupt network statistics or even disconnect large components of the community. Preceding node replication detection schemes depend mostly on centralized mechanisms with unmarried points of failure, or on neighborhood balloting protocols that fail to hit upon allotted replications. To deal with these essential boundaries, we advise new algorithms based on emergent properties [17], i.e., homes that stand up simplest thru the collective motion of multiple nodes. Randomized Multicast distributes node vicinity records to randomly-selected witnesses, exploiting the birthday paradox to locate replicated nodes, even as Line-selected Multicast uses the topology of the network to locate replication. Both algorithms provide globally-conscious, disbursed node-duplicate detection, and Line-selected Multicast displays especially strong overall performance characteristics. We display that emergent algorithms constitute a promising new technique to sensor community protection; furthermore, our results evidently expand to other classes of networks in which nodes may be captured, replicated and re-inserted through an adversary.

Random-walk based approach to detect clone attacks in wireless sensor networks
Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo and Li Xie-June 2010
The Wi-Fi sensor networks (WSNs) deployed in hostile environments is susceptible to clone assaults. In such attack, an adversary compromises a few nodes, replicates them, and inserts arbitrary quantity of replicas into the network. Therefore, the adversary can perform many inner assaults. Previous answers on detecting clone attacks have several drawbacks. First, a number of them require a imperative manage, which introduces several inherent limits. 2nd, a number of them are deterministic and susceptible to simple witness compromising attacks. 1/3, in a few answers the adversary can without problems research the important witness nodes to start smart assaults and guard replicas from being detected. In this paper, we first show that with the intention to avoid existing drawbacks, duplicate-detection protocols need to be non-deterministic and completely allotted (NDFD), and fulfill three security necessities on witness choice. To our knowledge, best one present protocol, Randomized Multicast, is NDFD and fulfills the necessities, but it has very excessive verbal exchange overhead. Then, based on random walk, we suggest new NDFD protocols,

Random stroll (RAWL) and desk-assisted Random walk (TRAWL), which fulfill the necessities whilst having simplest moderate verbal exchange and reminiscence overheads. The random stroll strategy outperforms previous techniques as it distributes a center step, the witness choice, to every exceeded node of random walks, after which the adversary cannot without difficulty discover the critical witness nodes. We theoretically examine the desired quantity of stroll steps for ensuring detection. Our simulation effects display that our protocols outperform an present NDFD protocol with the lowest overheads in witness choice, and TRAWL even has lower memory overhead than that protocol. The conversation overheads of our protocols are better however are less costly considering their security blessings.

Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks
Bo Zhu, Sajeev Setia, Sushil Jajodia, Sankardas Roy,Lingyu Wang-July 2010
Due to the negative physical protection of sensor nodes, it's far typically assumed that an adversary can seize and compromise a small quantity of sensors within the network. In a node replication assault, an adversary can take benefit of the credentials of a compromised node to surreptitiously introduce replicas of that node into the network. Without a powerful and green detection mechanism, these replicas can be used to release a selection of attacks that undermine many sensor applications and protocols. On this paper, we gift a novel distributed method referred to as Localized Multicast for detecting node replication assaults. The performance and security of our technique are evaluated both theoretically and via simulation. Our effects show that, compared to previous dispensed techniques proposed by means of Parno et al., Localized Multicast is greater green in phrases of conversation and reminiscence charges in massive-scale sensor networks, and on the identical time achieves a higher opportunity of detecting node replicas.

A Trigger Identification Service for Defending Reactive Jammers in Wireless Sensor Network
Ying Xuan,Yillin Shen,Nam P.Nguyen, My T.Thai-May 2012
In over the last decade, Reactive Jamming attack has emerged as a fantastic protection chance to wireless sensor networks, because of its mass destruction to valid sensor communications and difficulty to be disclosed and defended. Considering the particular characteristics of reactive jammer nodes, a brand new scheme to deactivate them by using successfully figuring out all trigger nodes, whose transmissions invoke the jammer nodes, has been proposed and developed. The sort of trigger-identification procedure can paintings as an utility-layer service and benefit many present reactive-jamming defending schemes. In this paper, on the only hand, we leverage several optimization issues to provide a whole trigger-identity provider framework for unreliable wireless sensor networks. However, we provide an improved algorithm with reference to 2 state-of-the-art jamming models, with the intention to enhance its robustness for diverse network scenarios.

A Bandwidth-Efficient Cooperative Authentication Scheme for Filtering Injected False Data in Wireless Sensor Networks
Rongxing Lu, Xiaodong Lin, Tom H. Luan, Xiaohui Liang, Xuemin (Sherman) Shen-Janauary 2012
Injecting false information attack is a widely known critical hazard to wireless sensor network, for which an adversary reviews bogus records to sink causing error selection at top stage and strength waste in en-course nodes. On this paper, we advise a novel bandwidth-green cooperative authentication (BECAN) scheme for filtering injected fake information. Primarily based at the random graph traits of sensor node deployment and the cooperative bit-compressed authentication approach, the proposed BECAN scheme can keep strength with the aid of early detecting and filtering the general public of injected fake records with minor more overheads on the en-path nodes. In addition, best a very small fraction of injected false facts wishes to be checked with the aid of the sink, which hence largely reduces the load of the sink. Both theoretical and simulation results are given to demonstrate the effectiveness of the proposed scheme in phrases of high filtering chance and strength saving.

Energy-efficient intrusion detection with a barrier of probabilistic sensors
Junkun Li, Jiming Chen, Ten H.Lai-March 2012
The Intrusion detection is a widespread utility in Wi-Fi sensor networks (WSNs). S. Kumar et al have brought the concept of barrier insurance, which deploys sensors in a narrow belt place to assure that any intrusion throughout the location is to be detected. But, the practical troubles have now not been investigated consisting of scheduling sensors strength-successfully even as making sure the detection possibility of any intrusion throughout the region based on probabilistic sensing model, that is a greater practical sensing version. Except, the intruders may be humans, animals, fighter planes or other things, which manifestly have diverse transferring speeds. On this paper, we examine the detection chance of arbitrary direction throughout the barrier of sensors theoretically and take

the maximum pace of feasible intruders into attention because the sensor networks are designed for one-of-a-kind intruders in distinct eventualities. Based at the theoretical evaluation of detection probability, we formulate a minimal Weight ∈-Barrier problem about the way to agenda sensors power-efficaciously. We display the problem NP-tough and advocate a bounded approximation algorithm, called minimal Weight Barrier set of rules (MWBA) to time table the activation of sensors. To evaluate our design, we analyze the overall performance of MWBA theoretically and also carry out good sized simulations to illustrate the effectiveness of our proposed algorithm.

IV. CONCLUSION

In this project, we have proposed distributed energy-efficient clone detection protocol with random witness selection. Specifically, we have proposed ERCD protocol, which includes the witness selection and legitimacy verification stages. Both of our theoretical analysis and simulation results have demonstrated that our protocol can detect the clone attack with almost probability 1, since the witnesses of each sensor node is distributed in a ring structure which makes it easy be achieved by verification message. In addition, our protocol can achieve better network lifetime and total energy consumption with reasonable storage capacity of data buffer.

This is because we take advantage of the location information by distributing the traffic load all over WSNs, such that the energy consumption and memory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended.

REFERENCES

[1] R. Lu, X. Li, X. Liang, X. Shen, and X. Lin, “GRS: The green, reliability, and security of emerging machine to machine communications,” IEEE Commun.Mag., vol. 49, no. 4, pp. 28–35, Apr. 2011.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” Comput. Netw., vol. 38, no. 4, pp. 393–422, Mar. 2002.

[3] A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, “Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks,” Comput. Netw., vol. 56, no. 7, pp. 1951–1967, May. 2012.

[4] T. Shu, M. Krunz, and S. Liu, “Secure data collection in wireless sensor networks using randomized dispersive routes,” IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[5] P. Papadimitratos, J. Luo, and J. P. Hubaux, “A randomized countermeasure against parasitic adversaries in wireless sensor networks,” IEEE J. Sel. Areas Commun., vol. 28, no. 7, pp. 1036–1045, Sep. 2010

[6] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, “Pseudonym changing at social spots: An effective strategy for location privacy in VANETs,” IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2012

[7] Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, “An early warning system against malicious activities for smart grid communications,” IEEE Netw., vol. 25, no. 5, pp. 50–55, May. 2011.

[8] R. Lu, X. Lin, X. Liang, and X. Shen, “A dynamic privacy-preserving key management scheme for location based services in VANETs,” IEEE Trans. Intell. Transp. Syst., vol. 13, no. 1, pp. 127–139, Jan. 2012

[9] M. Conti, R. D. Pietro, L. Mancini, and A. Mei, “Distributed detection of clone attacks in wireless sensor networks,” IEEE Trans. Dependable. Secure Comput., vol. 8, no. 5, pp. 685–698, Sep.-Oct. 2011.

[10] B. Parno, A. Perrig, and V. Gligor, “Distributed detection of node replication attacks in sensor networks,” in Proc. IEEE Symp. Security Privacy, Oakland, CA, USA, May. 8-11, 2005, pp. 49–63.

[11] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, “Random-walk based approach to detect clone attacks in wireless sensor networks,” IEEE J. Sel. Areas Commun., vol. 28, no. 28, pp. 677–691, Jun. 2010.

[12] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, “Localized multicast: Efficient and distributed replica detection in large-scale sensor networks,” IEEE Trans. Mobile Comput., vol. 9, no. 7,pp. 913–926, Jul. 2010.

[13] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, “A trigger identification service for defending reactive jammers in WSN,” IEEE Trans. Mobile Comput., vol. 11, no. 5, pp. 793–806, May. 2012

[14] R. Lu, X. Lin, H. Zhu, X. Liang, and X. Shen., “BECAN: A bandwidth-efficient cooperative authentication scheme for filtering injected false data in wireless sensor networks,” IEEE Trans.Parallel Distrib. Syst., vol. 23, no. 1, pp. 32–43, Jan. 2012

[15] J. Li, J. Chen, and T. H. Lai, “Energy-efficient intrusion detection with a barrier of probabilistic sensors,” in Proc. IEEE INFOCOM, Orlando, FL, USA, Mar. 25-30, 2012, pp. 118–126.