International Journal of Science Engineering and Advance Technology

A Distributed Clone Detection Protocol Considering Clone Detection Probability, Network Lifetime and Data Buffer Storage

[1*]S.Mani Karthik, [2]P.Rama Krishna
[1 2] Dept. of CSE, Kakinada Institute of Engineering & Technology, Korangi.

ABSTRACT:
We propose an energy-efficient location-aware clone location convention in thickly conveyed WSNs, which can ensure successful clone attack recognition and keep up attractive system lifetime. In particular, we misuse the area data of sensors and haphazardly select witnesses situated in a ring zone to check the authenticity of sensors and to report identified clone attacks. The ring structure encourages vitality productive information sending along the way towards the witnesses and the sink. We hypothetically demonstrate that the proposed convention can accomplish 100 percent clone identification likelihood with trustful witnesses. We additionally broaden the work by concentrate the clone identification execution with untrustful witnesses and demonstrate that the clone recognition likelihood still methodologies 98 percent when 10 percent of witnesses are traded off.

KEYWORDS: Wireless sensor networks, clone detection protocol, energy efficiency, network lifetime

I. INTRODUCTION:

Bargained accounts in Online Social Networks OSNs) are more good than Sybil records to spammers and different malicious OSN attackers. Malicious parties exploit the settled associations and trust connections between the honest to goodness account proprietors and their companions, and productively disseminate spam promotions, phishing joins, or malware, while abstaining from being hindered by the specialist co-ops. Disconnected examinations of tweets and Facebook posts uncover that most spam are appropriated through traded off records, rather than committed spam accounts. Late vast scale account hacking episodes in well-known OSNs additional proof this pattern. Not at all like devoted spam or sybil accounts, which are made exclusively to fill pernicious needs, bargained records are initially controlled by favorable clients, While committed malignant records can be essentially prohibited or expelled upon discovery, traded off records can't be taken care of similarly because of potential negative effect to ordinary client encounter (e.g., those records may in any case be effectively utilized by their genuine considerate proprietors). Major OSNs today utilize IP geolocation logging to fight against record compromisation. Nonetheless, this approach is known to experience the ill effects of low location granularity and high false positive rate.

LITERATURE SURVEY:

[1],we dissect the intrinsic elements, plan standards and assessment strategies for cost work based routing algorithms. Two vitality mindful cost based steering calculations named Exponential and Sine Cost Function based Route (ESCFR) and Double Cost Function based Route (DCFR) have been proposed in this paper. For ESCFR, its cost capacity can outline changes in nodal remaining vitality to extensive changes in the capacity esteem. For DCFR, its cost work mulls over the end-to-end energy utilization, nodal remaining vitality, bringing about a more adjusted and effective vitality use among nodes. The execution of the cost work configuration is dissected.

[2],we propose an area aware clone detection protocol, which ensures fruitful clone assault location and has minimal negative effect on the system lifetime. In particular, we use the area data of sensors and arbitrarily select witness hubs situated in a ring region to confirm the security of sensors and to distinguish clone assaults. The ring structure encourages vitality effective information sending along the way towards the witnesses and the sink, and the movement load is disseminated over the system, which enhances the system lifetime fundamentally. Hypothetical examination and recreation comes about exhibit that the proposed protocol can approach 100% clone discovery likelihood with trustful witnesses.

PROBLEM DEFINITION

To permit effective clone location, more often than not, an arrangement of hubs are chosen, which are called observers, to help confirm the authenticity of the hubs in the system. The private data of the source hub, i.e., character and the area data, is imparted to witnesses at the phase of witness choice. At the point when any of the hubs in the system needs to transmit information, it initially

sends the demand to the observers for authenticity confirmation, and witnesses will report a recognized assault if the hub falls flat the affirmation. To accomplish effective clone identification, witness choice and authenticity confirmation ought to satisfy two prerequisites: 1) witnesses ought to be haphazardly chosen; and 2) no less than one of the witnesses can effectively get all the check message(s) for clone recognition.

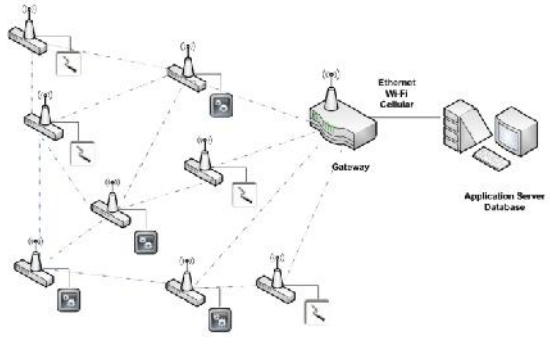
PROPOSED APPROACH

We find that the ERCD protocol can adjust the energy utilization of sensors at various areas by conveying the witnesses all over WSNs with the exception of non-witness rings, i.e., the neighboring rings around the sink, which ought not to have witnesses.

From that point forward, we acquire the ideal number of non-witness rings in view of the capacity of energy utilization.

At long last, we determine the statement of the required information cradle by utilizing ERCD protocol, and demonstrate that our proposed protocol is scalable in light of the fact that the required support storage is reliant on the ring size as it were.

SYSTEM ARCHITECTURE:



PROPOSED METHODOLOGY:

System Construction Module

We build up the System Construction Module, to assess and actualize our proposed framework. In this module, we consider a system area with one base station (BS) and a colossal number of remote sensor nodes arbitrarily conveyed in the system. We utilize the sink hub as the starting point of the framework facilitator. In view of the area of the BS, the system locale is for all intents and purposes isolated into neighboring rings, where the width of each ring is the same as the transmission scope of sensor hubs. The system is a thickly sent WSN, i.e., i) for every node, there exist sensor nodes situated in each neighboring ring, and ii) for each ring, in each ring, there are sufficient sensor nodes to develop a directing way along the ring.

ERCD Protocol

We introduce our distributed clone detection protocol, namely ERCD protocol, which can achieve a high clone detection probability with little negative impact on network lifetime and limited requirement of buffer storage capacity.

Probability of Clone Detection

We concentrate on outlining a conveyed clone detection protocol with arbitrary witness choice by mutually considering clone identification likelihood, arrange lifetime and information cradle stockpiling. At first, a little arrangement of hubs are traded off by the vindictive clients. Using the clone location protocol, we go for amplifying the clone discovery likelihood, i.e., the likelihood that cloned hub can be effectively identified, to guarantee the security of WSNs; in the mean time, the adequate vitality and cushion stockpiling limit with respect to information gathering and working clone recognition convention ought to be ensured, which implies that the system lifetime, i.e., the period from the begin of system operation until the principal blackout happens, ought not be affected by the proposed clone identification protocol with sensors' support storage.

Energy Consumption and Network Lifetime

In WSNs, since wireless sensor nodes are usually powered by batteries, it is critical to evaluate the energy consumption of sensor nodes and to ensure that normal network operations will not be broken down by node outage. Therefore, we define the network lifetime as the period from the start of network operation until any node outage occurs to evaluate the performance of the ERCD protocol.

ALGORITHM:

Notations:

ha The hop length from a to the sink
n The number of nodes in the network
ni The number of nodes in i-th ring
r The transmission range of a node
Oa The ring index of a
Owa The witness ring index of a
Wa The set of a's witness
wa One of a's witness in Wa
Sa The witness header of Wa
IDa The identity information of a
la The location a claims to occupy
ta The timer of a's verification
Ka The message including a's private information

DISTRIBUTED CLONE DETECTION PROTOCOL:

INPUT:HA,N,NI,R,KA

STEP1: witness selection, a random mapping function is employed to help each source node randomly select its
Witnesses.

STEP2: legitimacy verification, a verification request is sent from the source node to its

witnesses, which contains the private information of the source node.

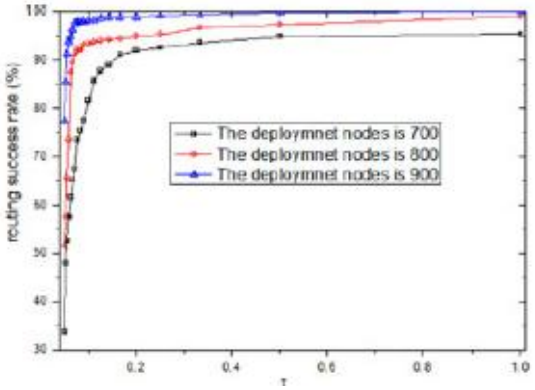
STEP3: If witnesses receive the verification messages, all the messages will be forwarded to the witness header for legitimacy verification.

STEP4: witness headers are nodes responsible for determining whether the source node is legitimacy or not by comparing the messages collected from all witnesses.

STEP5: If the received messages are different from existing record or the messages are expired.

STEP6: the witness header will report a clone attack to the sink to trigger a revocation procedure.

RESULTS:



Routing success rate with various duty cycle.

EXTENSION WORK:

The first proposal is based on a distributed hash table by which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes. Introducing new MAC Protocol along with distributed hash table which reduces energy consumption of sensors

CONCLUSION:

We have proposed circulated energy-efficient clone detection protocol with arbitrary witness determination. In particular, we have proposed ERCD protocol, which incorporates the witness choice and authenticity check stages. Both of our hypothetical investigation and recreation comes about have shown that our protocol can distinguish the clone assault with nearly likelihood 1, since the observers of every sensor hub is circulated in a ring structure which makes it simple be accomplished by confirmation message. Likewise, our protocol can accomplish better system lifetime and aggregate vitality utilization with sensible storage limit of information cushion. This is on account of we exploit the area data by circulating the movement stack all over WSNs, with the end goal that the vitality utilization and memory storage of the sensor nodes around the sink node can be alleviated and the system lifetime can be augmented.

REFERENCES:

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "ERCD: An energy-efficient clone detection protocol in WSNs," in Proc. IEEE INFOCOM, Apr. 14-19, 2013, pp. 2436–2444.

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

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

Mr.S.Mani Karthik is a student of Kakinada Institute of Engineering & Technology, Korangi. Currently, he is pursuing his M.Tech specializing in CSE department. He awarded his B.Tech specialized in CSE from Kakinada Institute of Engineering & Technology, Korangi.

Mr.Palli Ramakrishna, M.Tech is working as an Assistant Professor, Department of Computer Science and Engineering, at Kakinada Institute of Engineering and Technology, Korangi.