Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 4, Issue 1, January -2017

Energy Efficient Star Based Distribbuted Clone Detection In Wireless Ad-hoc Network

[1]Ms.Jigisha Bute, [2]Prof.D.O.Shamkuwar

[1,2]Dept Of Comp.Engg.Flora Institute Of Technology,Pune

Abstract — *Wireless device Networks (WSNs) square measure prone to clone attacks or node replication attacks as they're deployed in hostile and unattended environments wherever they're bereft of physical protection, lacking physical tamper-resistance of device nodes. As a result, associate mortal will simply capture and compromise device nodes and when replicating them, he inserts discretionary range of clones/replicas into the network. If these clones aren't expeditiously detected, associate mortal is more capable to mount a good form of internal attacks which might emasculate the assorted protocols and device applications. many solutions are planned within the literature to deal with the crucial downside of clone detection, that aren't satisfactory as they suffer from some serious drawbacks. during this paper we have a tendency to propose a unique distributed resolution known as Random Walk with Network Division (RWND) for the detection of node replication attack in static WSNs that relies on claimer-reporter-witness framework and combines a straightforward stochastic process with network division. RWND detects clone(s) by following a claimer-reporter-witness framework and a Random Walk is utilized inside every space for the choice of witness nodes. ripping the network into levels and areas makes clone detection additional economical and therefore the high security of witness nodes is ensured with moderate communication and memory overheads. Our simulation results show that RWND outperforms the present witness node primarily based ways with moderate communication and memory overheads.*

Keywords- *Wireless Sensor Networks, Clone Detection Protocol, Energy Efficiency, Network Lifetime, RWND.*

I. INTRODUCTION

Wireless detector Network (WSN) could be a assortment of detector nodes with powerful sensing capabilities however restricted resources. They comprises advanced network architectures and so square measure employed in a large style of applications. These sensors lack tamper resistance hardware due to value concerns and square measure typically deployed in powerful and rough settings and vicinities, hostile situations and unattended environments. Thus, they antagonize the extortions from the invaders and muggers which may launch several attacks as well as the intention to accumulate crucial data from the WSN or to enfeeble and enervate the tasks of the WSNs. Here, we have a tendency to notably specialise in additional harmful attack that is thought as node replication attack or clone attack. during this attack associate degree mortal physically captures one or additional detector nodes and compromise all its secret credentials. The node compromise consequently permits associate degree mortal to be capable of making clones or replicas of the compromised nodes so sneakily deploying them at strategic positions of the network.

An important distinctive behavior of clones or replicas is that they act as legitimate nodes or approved participants within the network. These clones have the cryptologic keying materials which permit them to appear like original legitimate detector nodes. Since, they behave honestly and participate within the network operations like non-compromised detector nodes so the legitimate and honest nodes don't seem to be alert to that there's a clone node among them. Consequently, all the prevailing authentication techniques and secure network communication protocols would simply permit these replicas to form combine wise shared keys with alternative nodes and also the base station, conjointly enabling them to encrypt/decrypt all their communications. If these clones don't seem to be detected with efficiency, fleetly and promptly, associate degree mortal will simply head of the network by exploiting these clones. Moreover, he/she will cripple several applications of the WSN because it terribly|is extremely|is incredibly} simple for him/her to compromise and replicate a typical detector node by employing a few without delay accessible tools during a very short amount of your time. Also, once associate degree mortal captures and compromises one detector node, it becomes the bottom to create clones and so the most value of attack is maintained. associate degree mortal may leverage these clones for launching several corporate executive attacks and malicious activities. for instance, he/she will produce a region, initiate a hole attack once many clones aggro up along, launch selective forwarding attack and DoS attack, inject false knowledge, monitor and take in good portion of traffic, denigrate and offend alternative nodes and even terminate legitimate nodes.

The most easy however unassertive answer to affect these clone node attacks is to equip the detector nodes with a tamper resistant hardware however this answer is inappropriate due to 2 main reasons; initial, it's uneconomical and extremely pricy to defend every of the detector nodes within the network with a tamper proof hardware, and second, it's going to still be potential to bypass tamper resistance for associate degree skilled assailant. Therefore, there's a necessity to develop code based mostly countermeasures for the detection of clone nodes. Within the literature 2 sorts of code based mostly solutions are projected for the detection of clone attack in static WSNs specifically Centralized and Distributed.

II. LITERATURE SURVEY

1) Paper Name: ERCD: An Energy-efficient Clone Detection Protocol in WSNs
Authors: Zhongming Zheng , Anfeng Liu , Lin X. Cai , Zhigang Chen , and Xuemin (Sherman) Shen
Wireless sensor networks (WSNs) play associate increasing role in a very large choice of applications starting from hostile atmosphere observation to telemedicine services. The hardware and value constraints of detector nodes, however, create sensors liable to clone attacks associated cause nice challenges within the style and readying of an energy-efficient WSN. during this paper, author propose a location-aware clone detection protocol, that guarantees flourishing clone attack detection and has very little negative impact on the network time period. Specifically, we tend to utilize the placement data of sensors and at random choose witness nodes placed in a very ring space to verify the privacy of sensors and to sight clone attacks. The ring structure facilitates energy economical information forwarding on the trail towards the witnesses and also the sink, and also the traffic load is distributed across the network, that improves the network time period considerably. Theoretical analysis and simulation results demonstrate that the projected protocol will approach 100 percent clone detection chance with credulous witnesses. we tend to additional extend the work by finding out the clone detection performance with untrustful witnesses and show that the clone detection chance still approaches ninety eight once 100 percent of witnesses are compromised. Moreover, our projected protocol will considerably improve the network time period, compared with the present approach.

2) Paper Name: GRS: The Green, Reliability, and Security of Emerging Machine to Machine Communications
Authors: Rongxing Lu, Xu Li, Xiaohui Liang, and Xuemin (Sherman) Shen
Machine-to-machine communications is characterised by involving an outsized range of intelligent machines sharing data and creating cooperative choices while not direct human intervention. thanks to its potential to support an outsized range of omnipresent characteristics and achieving higher value potency, M2M communications has quickly become a market-changing force for a good kind of period of time watching applications, like remote e-healthcare, good homes, environmental watching, and industrial automation. However, the flourishing of M2M communications still hinges on absolutely understanding and managing the present challenges: energy potency (green), dependableness, and security (GRS). while not bonded GRS, M2M communications can not be wide accepted as a promising communication paradigm. during this article, we tend to explore the rising M2M communications in terms of the potential GRS problems, ANd aim to market an energy-efficient, reliable, and secure M2M communications setting. Specifically, we tend to 1st formalize M2M communications design to include 3 domains — the M2M, network, and application domains — and consequently outline GRS necessities during a systematic manner. we tend to then introduce variety of GRS facultative techniques by exploring activity programing, redundancy utilization, and cooperative security mechanisms. These techniques hold promise in propulsive the event and preparation of M2M communications applications.

3) Paper Name: Wireless sensor networks: a survey
Authors: I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci
In this paper author describes the construct of detector networks that has been created viable by the convergence of micro-electro-mechanical systems technology, wireless communications and digital natural philosophy. First, the sensing tasks and also the potential detector networks applications ar explored, and a review of things influencing the planning of detector networks is provided. Then, the communication design for detector networks is made public, and also the algorithms and protocols developed for every layer within the literature ar explored. Open analysis problems for the conclusion of detector networks are mentioned. Recent advances in micro-electro-mechanical systems (MEMS) technology, wireless communications, and digital natural philosophy have enabled the event of low-priced, low-power, multifunctional detector nodes that are tiny in size and communicate unbound in brief distances. These little detector nodes, that contains sensing, processing, and human activity parts, leverage the thought of detector networks supported cooperative effort of an outsized range of nodes. detector networks represent a major improvement over ancient sensors.

4) Paper Name: Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks
Authors: Anfeng Liu a,b, Ju Ren a, Xu Li c, Zhigang Chen a, Xuemin (Sherman) Shen b
Cost operate based mostly routing has been wide studied in wireless detector networks for energy potency improvement and network period elongation. However, thanks to the complexness of the matter, existing solutions have numerous limitations. during this paper, we tend to analyze the inherent factors, style principles and analysis strategies for value operate based mostly routing algorithms. 2 energy aware value based routing algorithms named Exponential and circular function value operate based Route (ESCFR) and Double value operate based Route (DCFR) are planned during this paper. For ESCFR, its value operate will map little changes in nodal remaining energy to giant changes within the operate worth. For DCFR, its value operate takes into thought the end-to-end energy consumption, nodal remaining energy, leading to a a lot of balanced and economical energy usage among nodes. The performance of the price operate

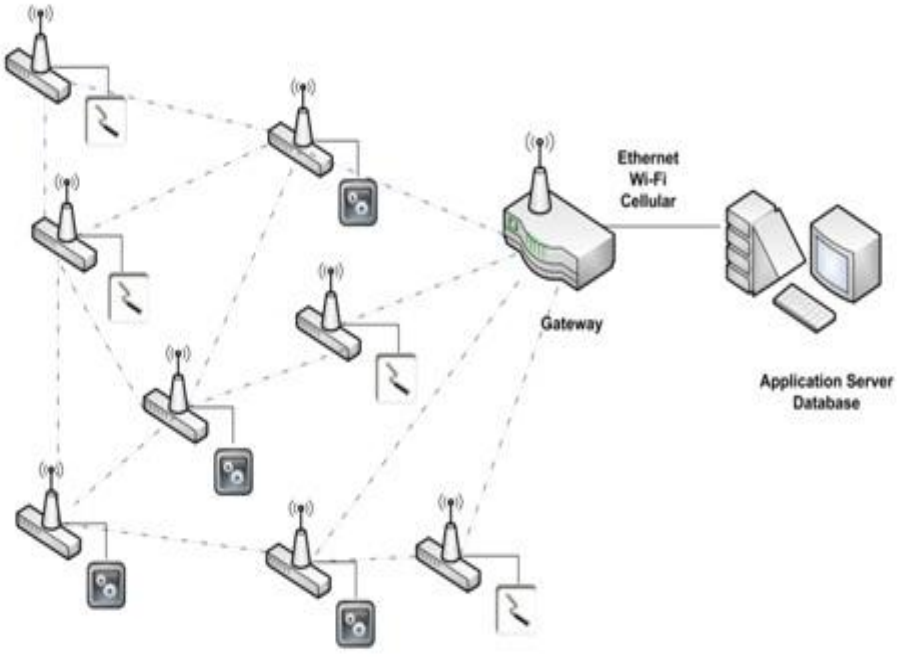
style is analyzed. in depth simulations demonstrate the planned algorithms have considerably higher performance than existing competitive algorithms.

5) Paper Name: Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive
Authors: Routes Tao Shu, Sisi Liu, and Marwan Krunz
Compromised-node and denial-of-service square measure 2 key attacks in wireless device networks (WSNs). during this paper, we have a tendency to study routing mechanisms that circumvent (bypass) black holes shaped by these attacks. we have a tendency to argue that existing multi-path routing approaches square measure at risk of such attacks, principally thanks to their settled nature. thus once associate resister acquires the routing formula, it will calculate an equivalent routes best-known to the supply, and thus endanger all info sent over these routes. during this paper, we have a tendency to develop mechanisms that generate randomised multipath routes. underneath our style, the routes taken by the “shares” of various packets amendment over time. thus even though the routing formula becomes best-known to the resister, the resister still cannot pinpoint the routes traversed by every packet. Besides randomness, the routes generated by our mechanisms are extremely dispersive and energy-efficient, creating them quite capable of bypassing black holes at low energy value. intensive simulations square measure conducted to verify the validity of our mechanisms.

III. PROPOSED SYSTEM

1. In this paper, besides the clone detection chance, we tend to conjointly contemplate energy consumption and memory storage within the style of clone detection protocol, i.e., associate energy- and memory-efficient distributed clone detection protocol with random witness choice theme in WSNs.
2. Our protocol is applicable to general densely deployed multi-hop WSNs, wherever adversaries might compromise and clone detector nodes to launch attacks.
3. We tend to extend the analytical model by evaluating the specified information buffer of ESCD protocol and by together with experimental results to support our theoretical analysis. Energy-Efficient Distributed Star based mostly Clone Detection (ESCD) protocol.
4. We discover that the ESCD protocol will balance the energy consumption of sensors at completely different locations by distributing the witnesses everywhere WSNs except non-witness distributed stars, i.e., the adjacent distributed stars round the sink, that mustn't have witnesses.
5. After that, we tend to acquire the best variety of non-witness distributed stars supported the perform of energy consumption.
6. Finally, we tend to derive the expression of the specified information buffer by mistreatment ESCD protocol, and show that our projected protocol is ascendible as a result of the specified buffer depends on the distributed star size solely.

IV. SYSTEM ARCHITECTURE



V. MATHEMATICAL MODEL

Let S be the whole System:

S= {N, CH, W, C}

Where,

1. N is the number of nodes
   N= {n1, n2, n3….n}

2. CH be the Cluster head
   CH= {ch1}

3. W be the Witness messages
   W= {w1, w2….wn}

4. C be the Clone nodes
   C={c1,c2,c3….cn}

Step 1: Node N will login into the system through ID and Password.

Step 2: After Login system S will authenticate the node.

Step 3: The Node will send the file to the database. When Node is sending file to database then at that time another node i.e. Clone node will also send the file.

Step 4: After receiving the files from Node and Clone node the system is requesting for Witness message.

Step 5: If the node will able to send the witness message then it is a valid node otherwise the clone is detected.

V. CONCLUSION

We have planned distributed energy economical clone detection protocol with random witness choice. Specifically, we've planned the ESCD protocol, which has the witness choice and legitimacy verification stages. additionally, our protocol are able to do higher network period and total energy consumption with cheap storage capability of knowledge buffer. The energy consumption and memory storage of the detector nodes round the sink node may be eased and therefore the network period may be extended.

VI. REFERENCES

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "ERCD: Anenergy-efficient clone detection protocol in wsns," in Proc. IEEE INFOCOM, Turin, IT, 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 emerging machine to machine communications," IEEE Communications Magazine, 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," Computer Networks, 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," Computer Networks, 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 Transactions on Mobile Computing, 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 Journal on Selected Areas in Communications, 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 Transactions on Vehicular Technology, 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 Network, 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 Transactions on Intelligent Transportation Systems, 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 Transactions on Dependable and Secure Computing, 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 Symposium on Security and 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 Journal on Selected Areas in Communications, 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 Transactions on Mobile Computing, vol. 9, no. 7, pp. 913–926, Jul. 2010.

[14] 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.

[15] T. Bonaci, P. Lee, L. Bushnell, and R. Poovendran, “Distributed clone detection in wireless sensor networks: An optimization approach,” in Proc. IEEE WoWMoM, Lucca, IT, Jun. 20-23 2011, pp. 1–6.

[16] B. Zhu, V. Addada, S. Setia, S. Jajodia, and S. Roy, “Efficient distributeddetection of node replication attacks in sensor networks,” in *Proc. 23rdAnn. Computer Security Applications Conference (ACSAC ’07)*, Dec. 2007, pp. 257–267.

[17] H. Choi, S. Zhu, and T. F. La Porta, “SET: Detecting node clones in sensor networks,” in *Proc. Third Int. Conf. Security and Privacy inCommunications Networks and the Workshops (SecureComm ’07)*, Sept. 2007, pp. 341–350.