DISTRIBUTED DIAGNOSIS OF CELLS ATTACKS IN THE WIRELESS SENSOR AND NETWORKS

K. Jegatha
M.Phil Computer Science
Noorul Islam Centre for Higher Education
Kumaracoil
Thuckalay-629180

Dr. J. R. Jeba
Associate Professor & HOD, Department of Computer Applications
Noorul Islam Centre for Higher Education
Kumaracoil
Thuckalay-629180

***Abstract*—** Wireless Sensor Networks (WSNs) are once in a while utilized in undermining conditions a foe can get a bit of the center points physically, promptly can reinvent, and after that, can duplicate them in countless, in this way assuming responsibility for the system. Some conveyed answers for handle this trouble have been as of late. These arrangements are not satisfactory. In the first place, the required more vitality also memory: A huge drawback for any procedure to be utilized in the WSN-resource constrained condition. Further, they are introduced to specific foe models appeared in this undertaking**.** To begin with, the properties of decentralized technique for the identification of hub Cells attacks are clarified. Second, surely understood answers for this issue which don't totally meet our necessities are clarified. Third, a novel self-retouching, Randomized, Efficient, and distributed (RED) method for the conspicuous verification of center Cells attacks**.** At last, recreation results demonstrate that our procedure is very efficient in correspondence, memory, also calculation; is significantly more accommodating than the arrangements clarified in the writing; is impervious to the new sort of attack showed in this endeavor, while different arrangements are definitely not.

Keywords - *Wireless sensor systems security, hub Cells attack identification, conveyed convention, strength, efficiency.*

1. INTRODUCTION

A Wireless Sensor System (WSN) was an aggregation of sensors with compelled resources that cooperate to achieve a Shared target. WSNs should be passed on in merciless circumstances to fulfil both military and normal Application [1] In light of time forward slanted to different kinds of novel attacks. For instance, an adversary could listen stealthily all framework trades; further, an enemy could discover centers securing every one of the information set away in that — sensors are routinely acknowledged to not cautiously structure. Thusly, an adversary might duplicate got sensors also send them in the structure to dispatch an assortment of compromising exercises. This attack is recommended as cell attack [11], [20]. Since a cell has authentic data (code and cryptographic material), it might investigate the system practices in like manner as a non-traded askew point; from this time forward cell focuses can dispatch an assortment of attacks. Two or three has been delineated in the creating [3], [7]. For example, a cell could make a diminish opening, start a wormhole trap with working together for or pervade false information or hard and fast information. In such an approach to managing tendency the final result [15]. Further, cells can spill information.

The threat of a cell ambush can be depicted by two essential concerns:

To have a lot of traded off focuses; the adversary do not have toward bargain a high number of focus focuses. Without a doubt, when a solitary focus point has been gotten and managed, the standard cost of the strike had been supported. Making further cells of an equivalent focus should be viewed as unassuming.

Towards the best of our comprehension, except for the convention proposed in [25] and watched out for in the running with, just bound together or near to customs have been proposed so far to conform to the cell attacks. While united customs have a solitary explanation behind disappointment and high correspondence cost, neighboring conventions don't perceive rehashed focuses that are passed on in various area of the structure. In this work search for a system self-correcting instrument, focus focuses independently see the closeness of cells and avoid them from any further structure action. Specifically, this instrument is intended to underline as a "customary practice" occasion: It is proposed for steady complement without significantly affecting the system shows while accomplishing high cell affirmation rate. In this paper take a gander at the engaging properties of dispersed parts for affirmation of focus Cells attacks [4]. In like way separate the first custom for orbited affirmation, proposed in [25], and demonstrate that this convention isn't totally engaging concerning the above properties. In the long run, pushed by [25], propose another randomized, efficient, and distributed (RED) custom for the affirmation of focus point cell attacks, and show that our convention meets all the above insinuate necessities. Further, give informative outcomes when RED and its rival face an adversary that expressly drops messages that could incite cell recognizing verification. At last, far-reaching ages of RED demonstrate that it is exceedingly efficient concerning exchanges, memory, and calculations required and show improved trap divulgence likelihood (regardless of when the foe is permitted to expressly drop messages) when showed up distinctively in connection to other appropriated customs. The straggling leftovers of this paper is made as looks for after Next piece audits related work; Segment III demonstrates the risk show expected in this paper; Segment IV displays the necessities a passed on convention for the affirmation of the cell attacks in remote sensor framework should meet; Segment V delineates our randomized, efficient, and orbited approach; Segment VI displays some test results on RED and contrast them and the outcomes got in [25] to the degree region likelihood, memory overhead, also centrality overhead. These outcomes confirm that RED matches the fundamentals set in Segment IV, that RED is more prominent importance, memory, and computationally efficient, also that it recognizes focus point cell attacks with a higher likelihood. In Segment, VII separate how noxious focus focuses can affect the affirmation convention shows.

2. RELATED WORKS

One of the first answers for the apperception of cell attacks depends upon an accumulated Base Station (BS) [24]. In this strategy, each inside point transfers a quick overview of its neighbors and their areas (that is the land orientation of middle) to a BS. A related focus ID in two records with conflicting domains will result in a cell apperception. By at that point, the BS denies the cells. This game-plan has two or three damages, for example, the propinquity of a solitary marker of disappointment (the BS) and high correspondence cost by virtue of the wide number of messages. Further, focus guides close toward the BS will be required to course fundamentally a bigger number of messages than different focuses, along these lines truncating their operational life.

The LSM tradition is identified with RM yet it exhibits a pivotal improvement to the extent area likelihood. In LSM, when a center point broadcasts its region, each neighbor first locally checks the characteristic of the case also thereafter, with likelihood p, propels it to g≥1 whimsically isolated objective centers. For example, in Figure 1 center point declares its zone and one of its neighbors, center b, advance the case to center f. A territory ensure, while peregrinating from source to objective, needs to experience a couple of middles of the street centers that structure the soi-disant ensure message way. In addition, each center that courses this case message needs to check the imprint, to store the message, also to check the clarity with the other zone claims got inside a comparable continue running of the disclosure tradition. Center is perceived by the center point (if present) on the intersection purpose of two different ways brought about by two assorted center point professes to pass on a comparative ID and oozing from two particular centers. In the point of reference showed up in Figure 1, center point cannot avoid being a cell of center an (it has a comparative ID of center a). The instance of $_{an}$ is transfer by center point c to center point e. In the model, center point it will by then outcomes in the union of two different ways passing on the instance of ID an emanating from different zones. Center point w, the eyewitness, perceives the aggressor and triggers a repudiation system. The purpose of increasing the ID likelihood is given by LSM. The essential beginning was towards reasonably segment the framework into cells also to consider all of the centers inside a cell as possible onlookers. In the first proposed tradition, Single Deterministic Cell, each center ID is identified with a lone cell inside the framework. Right, when the tradition runs, the neighbors of a center point a probabilistically transfer case to the single pre-chosen spectator cell for a. Once the first center point inside that cell gets the case information, the information is flooded to the different centers inside the cell. In the second recommendation, Parallel Multiple Probabilistic Cells, the neighbors of a center point a probabilistically transfer case to a subset of the pre-defined witness cells for a. The proposed game plans show higher recognizable proof likelihood appeared differently in relation to LSM.

3. SYSTEM ARCHITECTURE

The architecture diagram of opportunistic WSN is shown in Fig. 1

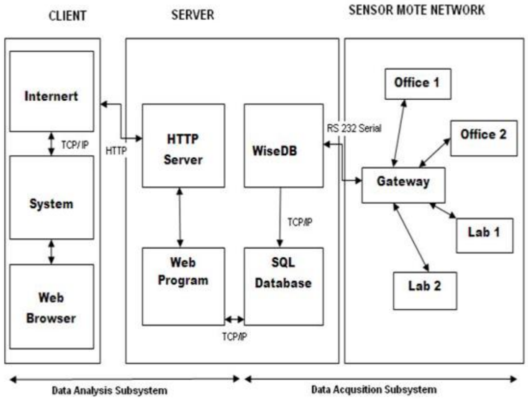

Fig.1. System Architecture

Another enamoring appropriated convention for repeated focus affirmation that has begun late been proposed is the SET custom [11]. SET use the information of sporadic respect passed on by a BS to play out a disclosure sort out. Specifically, the standard sporadic respect is first used to convey free social events and relating group heads. The specific packaging custom utilized guarantees that the get-togethers are in affirmation Exclusive Subset Maximal Independent Set (ESMIS) — gather heads are called Subset Leader (SLDRs). Further, inside a similar convention cycle used to make groups and SLDRs, no short of what one tree are defined over the structure diagram. The focuses of the tree relate towards the SLDRs. By at that point, a base up blend custom is hustled to mean the quick overview of focuses having a spot with the ESMIS. On the off chance that a middle ID is open in two unquestionable independent subsets than the inside point relating toward that inside ID had been a cell. The structure utilized by the custom keeps an inside point to circumvent recognizing confirmation by keeping up to be coordinated from a no existing SLDR—in this manner making tracks in a contrary course from the tree blend convention. Note that defining such assembling trees for every convention cycle run with a non-irrelevant cost like messages. Regardless, the fundamental issue of this custom is that the disclosure convention itself is flawed—it may be malevolently mishandled by the enemy to deny sensible focus focuses (that is, focus focuses that are not cell). When in doubt, a pernicious focus going about as an SLDR could proclaim in its ESMIS the closeness of an affirmed focus, express a, that as time goes on exists in some other piece of the structure (that is, having a spot with a substitute ESMIS). This pernicious direct will lead the structure to the "zone", and potentially to the refusal, of sensible focus a. In perspective on the likelihood of this snare, in the running with don't look at SET as a benchmark for our convention.

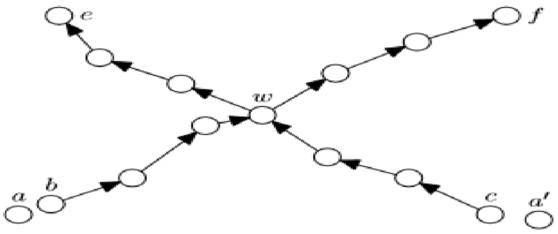

Fig: 2. LSM protocol iteration.

In [4] the creators raise the engaging properties a cell affirmation custom should meet. As appeared in [4], the LSM conventions [25] do not meet these properties. Specifically, in LSM two or three focus indicates have a higher likelihood go about as observers, so debilitating the distinctive verification itself. The aggressor can acknowledge responsibility for the inside that will keep running about as onlooker with most raised likelihood. Furthermore, the convention overhead isn't reliably passed on among the system focus focuses. In [5] a randomized, efficient and dissipated cell affirmation convention had been proposed. The redirection results separated in [5] demonstrate that the proposed RED Protocol meets the engaging properties appeared in [4]. Survey the obligation of [5] and further all around examine the likelihood

The examination and the further game plan of the re-enactments showed that the RED convention can be genuinely recognized in the form of a sensor. Moreover, research the impudence of an assailant interceding on message directing both for RED and LSM. Sometime the sending file content are chunk. When a file is send from the server, the file’s content may get corrupted or the content might be missed. That missed content will be retrieved and stored using RED Algorithm.

4. PROPOSED WORK

RED (Randomized Efficient and Distributed) another cell attacks region convention. RED is comparable on a fundamental measurement to the Randomized Multicast convention [25], yet with observers picked pseudo imprudently dependent on a system-wide seed. As a side-effect of the supposition that can efficiently pass. RED accomplishes a tremendous improvement over RM to the surviving correspondence and calculation. Precisely when separated and LSM [25], a custom that is more efficient than RM, RED breezes up being, once again, incredibly more noteworthy vitality efficient. More than that, in the running with domains, will display that RED is beside logically sound against an attacks that manhandles the uneven arrangement of spectators of LSM. Each keeps running of the custom includes two stages.

first step: An eccentric respect, and, is shared among the majority of the inside focuses. This emotional respect can be spoken with an assembled instrument (for instance, from a satellite or a UAV [16], or unmistakable sorts of ground-based focal stations), or with in-create spread structures. For example, a verified, verifiable pioneer race structure [6] should be utilized to pick a pioneer among the focuses; the pioneer will later pick and pass on the optional respect. In the straggling remains of this paper without loss of extensiv e clarification also to ease the work, it will depend on a united reaction to pass on the optional respect. In addition, this work recognizes that a substitute section is utilized to realize focus indicates not to lie about their physical zone.

In the second step, each inside point mindfully signs also locally confers its case—ID and geographic region (Procedure BROADCAST CLAIM in Protocol 1). Precisely when the neighbours get nearby by to pass on, the execute Procedure RECEIVE MESSAGE. The majority of the neighbors send (with likelihood p) the case to a lot of g≥1 pseudo-recklessly picked system domains (areas 4– 24 in Protocol 1). RED do not send the circumstance to a specific focus ID since this sort of answer does not scale well: A case send to a middle ID that isn't any inexorably present in the structure would be lost; fixates passed on after the first make course out of activity couldn't be utilized as spectators without resuscitating the majority of the focuses. Regardless, RED can without a considerable amount of a stretch be accustomed to working when a specific focus point is utilized as the message objective. At last, in the running with considering the equivalent geographic coordinating custom utilized in [25] for a reasonable examination. RED is, in reality, free of the controlling convention utilized in the system.

Expect that the guiding passes on a information send to a framework territory towards the center close to this zone [14] that the directing tradition do not bomb (as done in [25]); and, that information sending isn't impacted by dropping or wormhole attacks (for these sorts of attacks two or three game plans can be found in [3]). Similarly, acknowledge that the adversary can enrol the game plan of spectators. In any case, it can't speedily deal them since, when it moves to accomplish those centers, the tradition run submitted. Thereafter, in Section VII, will see how the tradition performs when pernicious centers should drop packs. Towards test the traditions, acknowledge that the foe has given two center points a comparative ID in the framework. Unquestionably, in case the foe exhibits more cells of a comparative center, by then the task of recognizing the attack is simply less requesting. Inside this ideal framework, the probability that the cell attack is distinguished is equal towards the probability that no short of what one neighbor of each cell transfer the case to comparative spectators. Considering d neighbours, the probability that from territory case information.

Every center signs its case information with its private key before imparting it (line 3 of Protocol 1). The center points that forward the checked case to objective are not required to add any signature or to store any information. Further, hand-off centers don't need to check the characteristic of the guided information: Signature looks openly be passed on by the objective simply—saving Θ (√n) signature checks per ensure send concerning LSM. Undoubtedly, while signature check at each center is basic in LSM for the distinguishing proof of the ambush, it isn't in RED. In any case, these checks should be useful in LSM to shield the enemy from making false information. In RED, if the adversary passes on region claims with false denotes, the genuine neighbors will by then forward the information all through the framework, also the horrendous mark won't be recognized until it accomplishes the recipient. This attack does not impact cell area itself—it will probably cripple the center points' battery. In this sense, this strike is out of the degree of this paper. In any case, in the going with the sketch a possible countermeasure: Relay centers should store a couple of bits as for send information so it is possible to pursue back the message originator if there ought to be an event of disillusionment of the imprinted check at the objective. Note that this countermeasure do not present a significant overhead.

Expect that the enemy cells personality IDA and commits this character to focus on. These two focus focuses are put in two obvious system regions: l1 and l2 independently. Amidst a RED highlight, the middle indicates need pass on a practically identical ID, exceptional region claims (l1 and l2). No ifs and's or buts, on the off chance that l1 ~l2, by then either the neighbors of the neighbors of a will raise a special case (line 14 of Protocol 1). Enable band c to be neighbors freely. Utilizing the pseudo-unusual farthest point both band c will pick a practically identical strategy of passerby focuses, containing something like a middle point w. Along these lines, will get a two confused area claims with character IDa—l1 and l2. This is outcome in cell affirmation. Thusly, I can begin a repudiation procedure for a focus point, Ida. Revocation should be performed by flooding the structure with the two confused cases gotten by w. Keep in mind that each case information of an inside point is separate with the private key of an equivalent focus point. Along these lines, the two cases are proof that Ida had been a cell. The custom shows one censure: After the rand respect is shared, RED enables the adversary to comprehend the onlooker set for some subjective ID. In any case, note that the onlookers of an inside point might be wherever in the structure and that watches change at each convention highlight eccentrically. This gathers the enemy, so as to shield RED from seeing the augmentations, is required to be incomprehensibly quick and to get the majority of the onlookers of the cells inside a window period that should beat most required between the presentation of rand also the finishing of the convention round. Considering sensible system sizes also the conceivable adversary speed, there are a couple of possible results for the foe to play out these attacks.

4.2 REQUIREMENTS FOR THE DISTRIBUTED DETECTION PROTOCOL

Around there present and legitimize the essentials that a tradition for cell area should meet.

A) Witness dispersion

A basic issue in sorting out a convention to see cell attacks is the confirmation of the onlookers. On the off chance that the foe knows the future onlookers before the conspicuous confirmation custom executes, the foe might subvert these middle focuses with the target that the snare goes undetected. The adversary can on a key measurement utilize any data on the system to anticipate likelihood $P_{witness}(s)$ for a nonexclusive focus point s. Here, have identified two sorts of wants: • ID-based check; • domain based want. Express that a convention for copy affirmation was ID missing if the customer do not give any data on the ID of the sensors that will be the observers of the cell snare amidst the going with the custom run. Consequently, a custom is a territory ignorant if likelihood $P_{witness}(s)$, for every sN, do not rely on the land position of focus point s in the structure.

B) Overhead:

Organizing customs for a remote sensor framework is an attempting errand because of the advantage requirements customary of these structures. Any convention is required to make inconsequential overhead. Regardless, this need alone isn't sufficient. In reality, paying little regard to whether a custom demonstrates a sensibly insignificant overhead on the common, it is as of recently conceivable that a little subset of the middle focuses encounters an essentially higher overhead. This is horrendous—these middle focuses exhaust their batteries all around rapidly, with genuine outcomes on the structure esteem. Also, the issue can be much logically subtle while thinking about memory. In the event that a high memory overhead focus on several inside focuses, by then these focuses should overflow. Amidst an overflow, the inside point might stop the convention, or drop packs to free memory. It is essential to get a handle on what sort of an effect this situation can have on the ID limit of the convention itself. can design the above contemplations with the general need that the overhead made by the custom ought to be near nothing, that is rational by the system when all is said in done, and (about) reliably dispersed among the inside focuses. To make an authentic model, in LSM each middle point that trades a position guarantee must play out an engraving verification also store the case. As investigated in [25], each line-section wires O (√n) focuses and each middle stores O (√n) domain claims. Note that this memory basic might be irrational in genuine structures with an extensive number of focus focuses. Table I appears—first push—the asymptotic overhead for one custom run (in addition recommended as round in the running with) of LSM.

C. Vitality overhead

To assess the essentialness overhead of the two traditions consider both correspondences also figuring heightened undertakings (that is, open key cryptography: signature age and imprint verification). In particular, using the essentialness IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING this article had been recognized for dissemination in a future issue of this journal yet had not been totally modified. The substance may change going before the last generation. Show proposed in [17]: A center point battery of 324,000 mg; 15.104 mg for transferring a package also 7.168 mg for getting a group (tolerating group length of 32 bytes, 0.059 mg for bit transferring and 0.028 mg for bit tolerating); and 25.0 mg for both imprint age also imprint verification.

D) Execution Evaluation

Red (Randomized Efficient and Distributed) another cells attack region convention. RED is close on a noteworthy measurement to the Randomized Multicast custom [25], yet with spectators picked pseudo-arbitrarily dependent on a system-wide seed. As a side-effect of the supposition that can efficiently circle the seed, RED accomplishes a liberal improvement over RM to the surviving correspondence and figuring. Precisely when separated and LSM [25], a custom that is more efficient than RM, RED winds up being, over again, incredibly more prominent importance efficient. More than that, in the running with segments, will show that RED is in like way powerfully historic against an attack that misuses the uneven dissipating of the proposed structure.

$$Pr[U]= Pr[U|Eh]Pr[Eh]+Pr[U|Em]Pr[Em].$$

Abstract respect, and, is shared among the majority of the inside focuses. This abstract respect can be spoken with the United system (for instance, from a satellite or a UAV [16], or different sorts of ground-based focal stations), or with in-make orbited portions. For example, an ensured, verifiable pioneer decision portion [6] can be utilized to pick a pioneer among the inside focuses; the pioneer will later pick and pass on the optional respect. In whatever is left of this paper, without loss of far-reaching decree also to ease working this work expect that a substitute system is utilized to keep up focus indicates not lie about their physical region. For instance, neighbor focuses can physically check the knowledge of the bore witness to zone. Such an immediate part, in like way utilized in [25], has the running with a downside: if the majority of the neighbors of a deceiving focus c1 are contaminated, they won't see c as a cheat. Thusly, this is a downside of both our custom and LSM.

$$\left[1+\frac{\binom{n-w}{\ell}}{\binom{n}{\ell}}\left(\frac{35}{36\pi^2}-\frac{1}{3}\right)\right]^i.$$

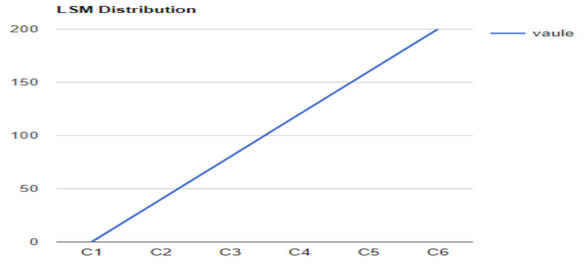

Fig. 3: Comparison of analysis of lifetime

In the second step, each inside mindfully signs also locally passes on its case ID and geographic region (Procedure BROADCAST CLAIM in Protocol 1). Precisely when the neighbors get the nearby by to grant, the execute Procedure RECEIVE MESSAGE. The majority of the neighbors send (with likelihood p) the case to a huge amount of g≥1 pseudo-capriciously picked structure domains (segments 4– 24 in Protocol 1). RED do not send the circumstance to a specific focus point ID since this sort of an answer does not scale well: A case send towards a middle ID that isn't any dynamically present in the structure would be lost; fixates passed on after the first sort out strategy couldn't be utilized as observers without resuscitating the majority of the inside focuses. Regardless, RED can without a great deal of a stretch be changed as per work when a specific focus point is utilized as the information objective. At last the running with considering the proportionate geographic planning convention utilized in [25] for a reasonable association. RED is amazingly free of the organizing convention utilized framework.

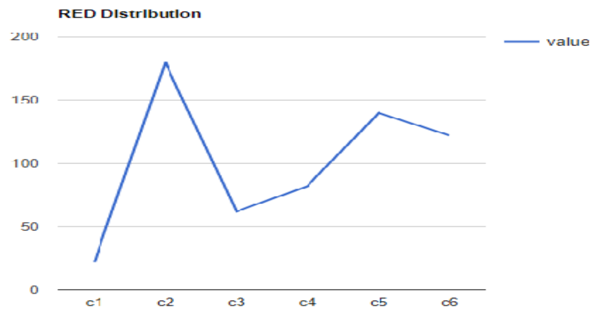

Fig.4: Comparison of analysis of packet delivery ratio

The veritable disclosure rate relies on a few elements like focus thickness, for instance. In any case, RED beats LSM even inside observing harmful hubs that can stop the convention. It is enrapturing to see how w and c influence the unmistakable verification likelihood. More noteworthy c proposes longer ways and a thus higher likelihood that one of the perilous focuses can stop cell divulgence.

$$1-\frac{1}{3}\left(1-\frac{35}{12\pi^2}\right)=\frac{1}{3}\left(2+\frac{35}{12\pi^2}\right).$$

Greater w infers that the adversary should often crush the traditions also influence area likelihood fundamentally, especially when c is huge. In all cases, clearly RED can meet to particularly high disclosure likelihood all around quickly. Note that RED is more influenced than LSM by route lengths since a dangerous center should stop the tradition wherever it appears in the ways. Regardless, tests show that for an arrangement of 1000 center points also correspondence run 0.1 in a framework region of IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING this article had been recognized for creation in a future issue of this journal yet had not been totally changed. The substance may change before indisputable creation. Side 1, c is about 0.35. Thusly, reason that RED had better recognizable proof likelihood also joins snappier than LSM for a each sensible estimation of the framework parameters.

6. CONCLUSION

Appeared and justified a few fundamental necessities a perfect custom for dispersed affirmation of focus copies ought to have. Specifically, have shown the key thought of ID-nonattendance and zone carelessness that pass on a degree of the possibility of the inside point augmentations territory convention; that is, its flexibility to a savvy foe. Besides, have displayed that the overhead of such a convention ought to be practically nothing, yet in addition reliably appropriated between the focuses, both in figuring also memory. Further, they had presented new enemy chance models. Regardless, a huge duty of this paper is fundamentally the proposal of a recouping, randomized, efficient, also surrounded convention (RED) to perceive focus point replication attacks. Effectively separated RED and the best level game-plan (LSM) also showed that the overhead presented by RED is low also reliably adjusted among the inside focuses; RED is both ID-reckless also zone indiscreet; likewise, RED beats LSM to the degree efficiency and adequacy. Wide diversion conform these outcomes. Considering, likewise inside observing traded askew focuses, can tentatively demonstrate that RED is more grounded in its affirmation limits than LSM.

7. REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey. International Journal of Computer and Telecommunications Networking – Elsevier”, Vol. 38(4),pp. 393–422, 2002.

[2] R. Brooks, P. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, “On the detection of clones in sensor networks using random key predistribution, IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews”, Vol. 37(6), pp. 1246–1258, 2007.

[3] M. Conti, R. Di Pietro, and L. V. Mancini, “ECCE: Enhanced cooperative channel establishment for secure pair-wise communication in wireless sensor networks`’, Ad Hoc Networks, Vol. 5(1), pp. 49–62, 2007.

[4] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, “Requirements and open issues in distributed detection of node identity replicas in WSN”,. In SMC ’06, pp. 1468–1473, 2006.

[5] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, “A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks”, In MobiHoc ’07, pp. 80–89, 2007.

[6] A. Derhab and N. Badache, “A self-stabilizing leader election algorithm in highly dynamic ad hoc mobile networks. IEEE Transactions on Parallel and Distributed Systems (TPDPS)”, Vol. 19(7), pp. 926–939, 2008.

[7] R. Di Pietro and L. V. Mancini, “Intrusion Detection Systems, Advances in Information Security”, Springer-Verlag, Vol. 38, 2008.

[8] R. Di Pietro, L. V. Mancini, and A. Mei, “Energy efficient nodeto-node authentication and communication confidentiality in wireless sensor networks. Wireless Networks, Vol. 12(6) pp. 709–721, 2006.

[9] R. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, “Playing hide-and-seek with a focused mobile adversary in unattended wireless sensor networks”, Ad Hoc Networks, Vol. 7(8), pp. 1463–1475, 2009.

[10] J. R. Douceur, “The sybil attack”, In IPTPS ’01, pp. 251–260. Springer, 2002.

[11] H. Choi, S. Zhu, and T. F. La Porta, “SET: Detecting Node Clones in Sensor Networks”, In SecureComm ’07, pp. 341–350, 2007.

[12] D. Dubhashi, O. H¨aggstr¨om, L. Orecchia, A. Panconesi, C. Petrioli, and A. Vitaletti, “Localized techniques for broadcasting in wireless sensor networks”, Algorithmica, Vol. 49(4)pp. 412–446, 2007

[13] J. Elson, L. Girod, and D. Estrin, “Fine-grained network time synchronization using reference broadcasts”, SIGOPS Operating Systems Review,Vol. 36(SI), pp. 147–163, 2002.

[14] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, “Highly-resilient, energy-efficient multipath routing in wireless sensor networks”, SIGMOBILE Mobile Computing and Communications Review, Vol. 5(4), pp. 11–25, 2001.

[15] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures”, Ad Hoc Networks,Vol. 1(2-3),pp. 293–315, 2003.

[16] J. Kong, H. Luo, K. Xu, D. L. Gu, M. Gerla, and S. Lu, “Adaptive Security for Multi-layer Ad-hoc Networks”, Special Issue of Wireless Communications and Mobile Computing, Wiley Interscience Press, Vol. 2(5), pp. 533–547, 2002.

[17] Q. Zhang, T. Yu, and P. Ning, “A framework for identifying compromised nodes in wireless sensor networks.

ACM Transactions on Information and System Security (TISSEC)", Vol. 11(3), pp. 1–37, 2008.

[18] S. Kwon and N. B. Shroff, "Catch 22 of Shortest Path Routing for Large Multi-Hop Wireless Networks", Vol. 4(7), pp. 568-579, 2007

[19] Jiejun Kong and HaiyunLuo and KaixinXu and Daniel LihuiGu, "Versatile Security for Multi-layer Ad-hoc Networks", Vol. 23, pp. 211-225, 2007

[20] F. Fu, J. Liu, and X. Yin , "Space-Time Related Pairwise Key Predistribution Scheme for Wireless Sensor Networks", Vol. 4(11), pp. 2692-2696, 2007

[21] D. Ganesan and R. Govindan and S. Shenker and D. Estrin, "Profoundly Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks", Vol. 53(11), pp. 45-433, 2001.

[22] Dr.M. Preetha1, K. Sivakumar , "An Energy Efficient Sleep Scheduling Protocol for Data Aggregation in WSN", Vol. 27(14), pp. 574-589, 2003.

[23] K. Johny Elma and Dr.S. Meenakshi., "Vitality Efficient Clustering for Lifetime Maximization and Routing in WSN", Vol. 15(9), pp. 349-362, 2008

[24] L.Eschenauer ana V.D. Gligor, "A key-management scheme for distributed sensor networks", In CCS 02, pp. 41-47, 2002.

[25] B. Parno, A. Perrig, and V.D. Gligor, "Distributed detection of node replication attacks in sensor networks", In S&P 05, pp. 49-63, 2005.