A MISBEHAVIOUR NODE DETECTION SCHEME FOR WIRELESS SENSOR NETWORKS

1.S.Gowri,2.M.Kamarunisha, 3. A.Sivasankari
Asst. professors, Department of computer Applications, Dhanalakshmi Srinivasan College of Arts and Science for Women (Autonomous),Perambalur.

ABSTRACT

Security is one of the primary issues that have pulled in a huge load of creative work effort as of late. In multi-ricochet far off improvised association interface botch and pernicious group dropping are two hotspots for package mishaps. Whether or not the adversities are achieved by associate bungles only, or by the merged effect of association botches and toxic drop are to be perceived, can be known by seeing a progression of bundle mishaps in the association. Regardless, in the insider-attack case, whereby poisonous center points that are significant for the course abuse their knowledge into the correspondence setting to explicitly drop a restricted amount of packages essential to the association execution. Ordinary figuring's that rely upon recognizing the pack mishap rate can't achieve adequate area accuracy considering the way that the package dropping rate for the present circumstance is equivalent to the channel botch rate. In this way to assemble the distinguishing proof precision in the group setback information declared by centers. This system gives assurance defending, scheme affirmation, and achieves low correspondence and limit overheads. A group block based framework is moreover proposed, to diminish the computation overhead of the example contrive, which grants one to trade acknowledgment accuracy for lower estimation multifaceted nature

KEYWORDS: Information security, wireless sensor networks, event detection, continuous wavelet transforms

INTRODUCTION

Distant Sensor Networks (WSNs), prodded by military applications, security has been a huge concern. Nowadays, WSNs are notable for IoT applications, for instance, savvy metropolitan regions, splendid structures and clinical consideration, anyway security risks could at present stance costly and even dangerous issues. WSNs are normally introduced to genuine shortcomings, since they are every now and again truly open, unattended, and unendingly creating considering sensors joining and leaving the association. What's more, the usage of security instruments, for instance, complex cryptographic frameworks is bound because of computational restrictions. In like manner, the cost of mishandling such shortcomings is less an obstruction for malicious activities. In particular, the assessments' decency may be blocked: we suggest this attack as toxic data implantations. Regardless, when ordinary security parts are set up, they can't prevent a bit of the attacks. In particular, an attacker can regulate the WSN by really modifying sensor contraptions or controlling the atmosphere itself. In a couple of circumstances, these can't be prevented with proactive security instruments. For example, metropolitan traffic sensors may be deliberately uneven at the time they are implanted to calm alerts for road incidents. In such cases, the just mean to kill malignant data implantations is revelation through examination of the assessments themselves

This is possible because of between assessments

relationship. Connections exist between assessments of different sensors across the WSN space, which we imply as spatial association. Associations moreover exist across the assessments of a comparative sensor true to form, known as momentary connections, and between various noticed miracles, known as quality connections. Right when spatial associations are changed, they give verification of inconsistencies between sensors, which are likely going to happen when legitimate and threatening sensors correspond. Spatial relationship enables distinguishing proof just if the assessments from a subset of sensors are extensively changed. This assumption that is generally genuine since the aggressor's cost and risk for changing assessments of more sensors increases moderately with their number. All things considered, transient relationship fails to uncover dangerous data if the attacker adjusts even a single sensor and applies a smooth advancement among affirmed and noxious data. The significant doubt for the fittingness of property association is that the sensor center points screen various wonders, and one of them isn't sabotaged. In any case, as various sensors are related with a comparative sensor center point, changing it engages the aggressor to control all the noticed wonders. The chance of recognizing toxic data mixtures depends upon the ability to mishandle association similarly as on the attack's intricacy. We imagine that toxic assessments can be imbued with any intricate method that intensifies the damage to the WSN and limits the threat of being recognized.

This is possible at whatever point compromised centers scheme, i.e., act in show towards a shared goal. The issue ends up being impressively all the all the more testing when events occur in the noticed genuine marvel. Savage blasts are a delineation of event for temperature checking WSNs, while tremors are an outline of event for seismic WSNs. The effect of events is to change the assessments connections, especially when seen just by a subset of sensors. This genuine change in relationship can be manhandled by an advanced attacker to legitimize the association corruption got by malicious data. We propose a technique for recognizable proof of malicious data implantations inside seeing present day course of action approaches, considering a cross-scale assessment of the wavelet change applied to the assessments in the spatial space. Anyway we highlight that perceiving anomalies in the assessments isn't satisfactory to effectively adjust them. The adjustments in the vindictive assessments and the impacted sensors should be recognized. We imply this endeavor as depiction. Also, we deal with the finding of the recognized abnormalities. Indeed, genuine faults may in like manner present peculiarities, as the assessments from flawed sensors don't compare with those of sound ones. This may incite some unsuitable end that there was an attack, anyway by orchestrating the guideline ascribes of authentic defects we can infer when the peculiarity is without a doubt pernicious.

ISSUES AND CHALLENGES

The issue ends up being logically confusing as the amount of pernicious sensors increases. Right when the attacker's capacities are enough high, the assailant may successfully reproduce genuine events without setting off acknowledgment or make threatening sensors be recognized as confirmed, and genuine sensors as malignant. The issue ends up being a lot of all the additionally testing when events occur in the checked real marvel. Crazy flames are an outline of event for temperature checking WSNs. Regardless, when essential security parts are set up, they can't hinder a bit of the attacks. In particular, an attacker can direct the WSN by truly changing sensor devices or controlling the atmosphere itself. In a couple of circumstances, these can't be thwarted with proactive security segments.

MOTIVATION

In the proposed to distinguish traditional idiosyncrasies rather than purposeful noxious implantations, so they are not planned to adjust to understanding, this fundamentally lessens the chances of revelation. Likewise, the assessments scattering is normal homogeneous and this doubt doesn't hold especially when explicit events of interest occur, for instance, wild flames, quakes, psychotic conditions, etc The basic idea of trust the heads strategies is to screen a sensor's cooperation true to form, selecting it a trust regard, which is persistently revived. This should be conceivable by mishandling a typical assessments course, or checking if a sensor precisely reports the presence of events of income. The information of sensors with a low trust regard is seen as less strong, in this manner the impact of noxious data is decreased.

RELATED WORKS

In [1] M. Ameen, J. Liu, and K. Kwak et al presents The use of distant sensor associations (WSN) in clinical consideration applications is filling in a brisk development. Different applications, for instance, beat screen, circulatory strain screen and endoscopic case are as of now being utilized. To address the creating usage of sensor advancement here, another field known as distant body an area associations (WBAN or simply BAN) has emerged. As most devices and their applications are far off in nature, security and assurance concerns are among critical regions of concern. Due to coordinate consideration of individuals also grows the affectability. Whether or not the data amassed from patients or individuals are gotten with the consent of the individual or without it due to the need by the structure, misuse or security concerns may restrict people from abusing the full points of interest from the system. People may not see these devices okay for step by step use. There may moreover likelihood of certifiable social strife due to the fear that such devices may be used for noticing and following individuals by government workplaces or other private affiliations. In this papeSensor networks are being used in a wide extent of utilization zones. The critical application spaces we analyze these issues and dismember in detail the issues and their potential measures are Home and office, control and robotization, collaborations and transportation, natural checking, clinical consideration, security and observation, the movement business and entertainment, tutoring and getting ready and redirection. Sensor contraptions that can be used to screen human activities have procured staggering assessment expense recently are home and office, control and computerization, collaborations and transportation, normal noticing, clinical administrations, security and perception, the movement business and unwinding, tutoring and getting ready and entertainment.

In [2] M. Li, W. Lou, and K. Ren et al presents another innovation for e-medical care that permits the information of a patient's fundamental body boundaries and developments to be gathered by little wearable or implantable sensors and conveyed utilizing short-range remote correspondence methods. WBAN has indicated extraordinary potential in improving medical services quality, and accordingly has discovered a wide scope of utilizations from omnipresent wellbeing checking and PC helped restoration to crisis clinical reaction frameworks. The security and protection assurance of the information gathered from a WBAN, either while put away inside the WBAN or during their transmission outside of the WBAN, is a significant unsolved worry, with challenges coming from rigid asset requirements of WBAN gadgets, and the appeal for both security/security and common sense/ease of use. In this article we investigate two significant information security issues: secure and reliable appropriated information stockpiling, and fine-grained conveyed information access control for delicate and private patient clinical information. We talk about different reasonable issues that should be considered while satisfying the security and protection necessities. Significant arrangements in sensor organizations and WBANs are studied, and their appropriateness is dissected. The quick improvement in wearable clinical sensors and remote correspondence, remote body zone organizations (WBANs) have arisen as a promising strategy that will revolutionalize the method of looking for medical care, which is regularly named e-medical services. Rather than being estimated vis-à-vis, with WBANs patients' wellbeing related boundaries can be observed distantly, ceaselessly, and progressively, and afterward handled and moved to clinical information bases. This clinical data is divided between and gotten to by different clients, for example, medical services staff, specialists, government offices, and insurance agencies.

In [3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami et al presents Ubiquitous detecting empowered by Wireless Sensor Network (WSN) innovations cuts across numerous zones of advanced living. This offers the capacity to quantify, deduce and comprehend ecological pointers, from sensitive ecologies and common assets to metropolitan conditions. The expansion of these gadgets in an imparting inciting network makes the Internet of Things (IoT), wherein sensors and actuators mix flawlessly with the climate around us, and the data is shared across stages to build up a typical working picture (COP). Filled by the new variation of an assortment of empowering remote innovations, for example, RFID labels and installed sensor and actuator hubs, the IoT has ventured out of its outset and is the following progressive innovation in changing the Internet into a completely coordinated Future Internet. As we move from www (static pages web) to web2 (interpersonal interaction web) to web3 (omnipresent registering web), the requirement for information on-request utilizing modern instinctive inquiries increments essentially. This paper presents a Cloud driven vision for overall usage of Internet of Things. The key empowering advances and application spaces that are probably going to drive IoT research sooner rather than later are examined. A Cloud execution utilizing Aneka, which depends on cooperation of private and public Clouds, is introduced. We finish up our IoT vision by developing the requirement for assembly of WSN, the Internet and circulated registering coordinated at innovative examination network. The following wave in the time of registering will be external the domain of the customary work area. In the Internet of Things (IoT) worldview, a large number of the articles that encompass us will be on the organization in some structure

In [4] C. Karlof and D. Wagner et al presents the directing security in remote sensor organizations. Numerous sensor network directing conventions have been proposed, however none of them have been planned with security as an objective. We propose security objectives for steering in sensor organizations, show how assaults against impromptu and distributed organizations can be adjusted into incredible assaults against sensor organizations, present two classes of novel assaults against sensor organizations – sinkholes and HELLO floods, and break down the security of all the significant sensor network directing conventions. We depict devastating assaults against every one of them and propose countermeasures and plan contemplations. This is the primary such examination of secure steering in sensor organizations. Our attention is on steering security in remote sensor organizations. Current proposition for directing conventions in sensor networks upgrade for the restricted capacities of the hubs and the application explicit nature of the organizations, yet don't think about security. In spite of the fact that these conventions have not been planned with security as an objective, we feel it is imperative to dissect their security properties. At the point when the safeguard has the liabilities of unreliable remote correspondence, restricted hub capacities, and conceivable insider dangers, and the foes can utilize amazing workstations with high energy and long reach correspondence to assault the organization, planning a safe steering convention is non-inconsequential One part of sensor networks that convolutes the plan of a protected directing convention is in-network conglomeration. In more traditional net Message trustworthiness, genuineness, and classification are taken care of at a higher layer by a start to finish security instrument. In-network handling makes start to finish security instruments more enthusiastically to convey on the grounds that middle hubs need direct admittance to the substance of the messages. Connection layer security systems can help intercede a portion of the subsequent weaknesses.

In [5] A. Perrig, J. Stankovic, and D. Wagner et al presents Recent advances in hardware and remote correspondence advances have empowered the improvement of enormous scope remote sensor networks that comprise of some low-powers, minimal effort and little size sensor hubs. Sensor networks hold the guarantee of encouraging huge scope and constant information handling in complex conditions. Security is basic for some, sensor network applications, for example, military objective following and security observing. To give security and protection to little sensor hubs is trying, because of the restricted abilities of sensor hubs regarding calculation, correspondence, memory/stockpiling, and energy supply. In this article we overview the cutting edge in exploration on sensor network security. Remote sensor networks have applications in numerous significant zones, for example, the military, country security, medical care, the climate, agribusiness, and assembling. One can imagine later on the organization of huge scope sensor networks where hundreds and thousands of little sensor hubs structure self-coordinating remote organizations. Giving security in sensor networks is certainly not a simple undertaking. Contrasted with ordinary work stations, serious limitations exist since sensor hubs have restricted handling capacity, stockpiling, and energy, and remote connections have restricted data transmission. Regardless of the previously mentioned difficulties, security is significant and even basic for some utilizations of sensor organizations, for example, military and country security applications. A few ongoing commitments to the writing have tended to security and protection issues in sensor organizations. In this article we talk about flow and past examination exercises did on sensor network security.

BACKGROUND PROCESS PACKET DROPPING

Bundle misfortune happens when at least one parcels of information traversing a PC network neglect to arrive at their objective. Bundle misfortune is regularly brought about by network clog. Bundle misfortune is estimated as a level of parcels lost concerning parcels sent. Parcel misfortune happens when at least one bundles of information bridging a PC network neglect to arrive at their objective. Bundle misfortune is regularly brought about by network clog. Parcel misfortune is estimated as a level of bundles lost regarding parcels sent. The Transmission Control Protocol (TCP) identifies bundle misfortune and performs retransmissions to guarantee solid informing. Parcel misfortune in a TCP association is additionally used to dodge clog and subsequently delivers a deliberately decreased throughput for the association

ROUTING PROCESS

Organization examination is the way toward finding the voltages across, and the flows through, each segment in the organization. There are various procedures for ascertaining these qualities. In any case, generally, the applied method expects that the segments of the organization are altogether straight. The techniques portrayed in this article are simply pertinent to straight arrange investigation, aside from where expressly expressed.

PACKET TRANSMISSION

In the wake of finishing the arrangement stage, S enters the bundle transmission stage. S sends bundles to PSD as indicated by the accompanying advances. Prior to conveying a bundle Pi, where I is a succession number that remarkably distinguishes Pi, S figures and creates the HLA marks of ri for hub nj, as follows the hub has gotten, and it transfers to the following jump on the course. The last bounce, i.e., hub nK, just advances Pi to the objective D. As demonstrated in Theorem 4 in Section 4.3, the extraordinary structure of the single direction fastened encryption development in (4) directs that an upstream hub on the course can't get a duplicate of the HLA signature planned for a downstream hub, and consequently the development is versatile to the arrangement model characterized in Section 3.2. Note that here we consider the confirmation of the uprightness of Pi as a symmetrical issue to that of checking the tag tji. On the off chance that the confirmation of Pi fizzles, hub n1 ought to likewise quit sending the bundle and should stamp it appropriately in its evidence of-gathering information base.

WORKING PROCESS

- Set Up Phase
- Packet Transmission Phase
- Audit Phase
- Detection Phase

Set Up Phase

This stage happens just after course PSD is set up, yet before any information parcels are sent over the course. In this stage, S chooses a symmetric-key crypto-framework scramble key; unscramble key and K symmetric keys key1; . . . ; key K, where encode key and decode key are the keyed encryption and unscrambling capacities, individually. S safely disperses decode key and a symmetric key j to hub nj on PSD, for j ¼ 1; . . .;K. Key dispersion might be founded on the public-key crypto-framework, for example, RSA: S scrambles keyj utilizing the public key of hub nj and sends the code text to nj. nj unscrambles the code text utilizing its private key to get keyj. S additionally reports two hash capacities, H1 and HMAC key, to all hubs in PSD. H1 is unkeyed while HMAC key is a keyed hash work that will be utilized for message validation purposes later on. Other than symmetric key dissemination, S likewise needs to set up its HLA keys.

Packet Transmission Phase

Subsequent to finishing the arrangement stage, S enters the bundle transmission stage. S sends parcels to PSD as indicated by the accompanying advances. Prior to conveying a bundle Pi, where I is a succession number that interestingly distinguishes Pi, S processes and produces the HLA marks of ri for hub nj, as follows the hub has gotten, and it transfers to the following bounce on the course. The last bounce, i.e., hub nK, just advances Pi to the objective D. As demonstrated in Theorem 4 in Section 4.3, the exceptional structure of the single direction binded encryption development in (4) directs that an upstream hub on the course can't get a duplicate of the HLA signature proposed for a downstream hub, and hence the development is tough to the plot model characterized in Section 3.2. Note that here we consider the confirmation of the honesty of Pi as a symmetrical issue to that of checking the tag tji. In the event that the check of Pi falls flat, hub n1 ought to likewise quit sending the parcel and should stamp it appropriately in its evidence of-gathering information base.

Audit Phase

This stage is set off when the public reviewer Ad gets an ADR message from S. The ADR message remembers the id of the hubs for PSD, requested in the downstream course, i.e., n1; . . . ; nK, S's HLA public key data, the grouping quantities of the latest M bundles sent by S, and the arrangement quantities of the subset of these M parcels that were gotten by D. Review that we accept the data sent by S and D is honest, in light of the fact that recognizing assaults is to their greatest advantage. Advertisement leads the evaluating cycle as follows. Promotion presents an arbitrary test where the components cji's are arbitrarily browsed Zp. Without loss of consensus, let the grouping number of the bundles recorded in the current verification of-gathering information base be P1; . . . ; PM, with PM being the latest bundle sent by S. the above instrument just ensures that a hub can't downplay its parcel misfortune, i.e., it can't guarantee the gathering of a bundle that it really didn't get. This component can't keep a hub from excessively expressing its bundle misfortune by asserting that it didn't get a parcel that it really got.

Detection Phase

The public inspector Ad enters the location stage in the wake of accepting and reviewing the answer to its test from all hubs on PSD. The fundamental assignments of Ad in this stage incorporate the accompanying: distinguishing any exaggeration of bundle misfortune at every hub, developing a parcel misfortune bitmap for each jump, figuring the autocorrelation work for the bundle misfortune on each bounce, and choosing whether pernicious conduct is available.

Given the bundle gathering bitmap at every hub, b1; . . . ; ~b K, Ad first checks the consistency of the bitmaps for any conceivable exaggeration of bundle misfortunes. Unmistakably, in the event that there is no exaggeration of parcel misfortune, at that point the arrangement of bundles got at hub j þ 1 should be a subset of the parcels got at hub

j. Since an ordinary hub in every case honestly reports its parcel gathering, the bundle gathering bitmap of a malevolent hub that exaggerates its parcel misfortune should negate with the bitmap of a typical downstream hub. Note that there is consistently in any event one ordinary downstream hub, i.e., the objective D. So Ad just necessities to consecutively check ~bj's and the report from D to distinguish hubs that are exaggerating their bundle misfortunes

ALGORITHM

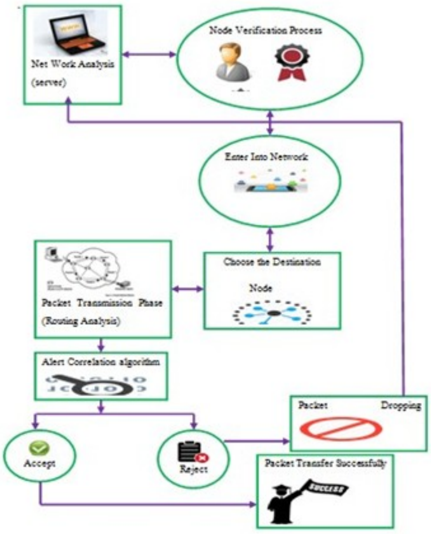
MULTI-FACTOR AUTHENTICATION

Multifaceted confirmation (additionally MFA, Two-factor verification, TFA, T-FA or 2FA) is a way to deal with validation which requires the introduction of at least two of the three confirmation factors: an information factor ("something just the client knows"), a belonging factor ("something just the client has"), and an inherence factor ("something just the client is").

ALERT CORRELATION

Ready Correlation calculation is followed for each alarm distinguished and returns at least one ways Si. For each ready ac that is gotten from the IDS, it is added to ACG in the event that it doesn't exist. For this new ready ac, the comparing vertex in the SAG is found by utilizing capacity map.

ARCHITECTURE DIAGRAM


Net Work Analysis (server)
Node Verification Process
Enter Into Network
Choose the Destination Node
Packet Transmission Phase (Routing Analysis)
Alert Correlation algorithm
Packet Dropping
Accept
Reject
Packet Transfer Successfully
SUCCESS

In the organization investigation, the hubs can be register and gone into network, after login measure every hub can be confirmed. During the transmission Phase every hub can be checked if the phony hub is showed up methods utilizing the ready relationship calculation created the caution and alarm the leftover hub.

RESULT AND DISCUSSION

A sensor node is compromised randomly by the attacker at a specific probability every cycle, referred to as the attack probability, and then this malicious node keeps reporting the opposite information after compromised. For example, a malicious node always sends “alarm” while the aggregation result computed from other sensor nodes is “no alarm”. Meanwhile, a normal sensor node may also send alarm when real alarm occurs. This case also occurs randomly at a different alarm probability.

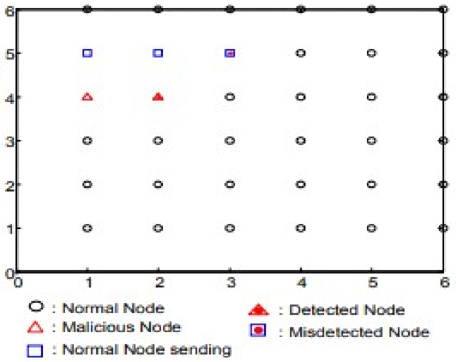


Fig sensor nodes deployment in the simulation

Under the assumption that sensor nodes are densely deployed to monitor certain target. In contrast to malicious nodes, if a normal node started sending alarm, its neighbor nodes would also start to send alarm after a short delay time. Furthermore, normal alarming nodes will stop sending alarms after a certain cycles. The node, which is detected or misdetected as a malicious node, is inactivated from the whole processing. The detection is terminated after 200 cycles or more than 25% of all nodes are detected as malicious nodes. Each result is calculated form an average over 1000 independent simulations

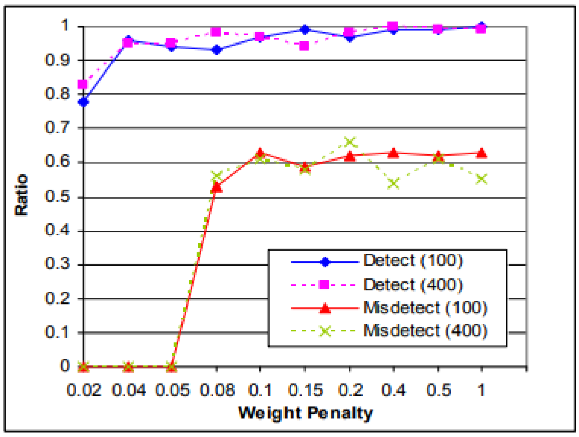


Fig Penalty Weights on system performance

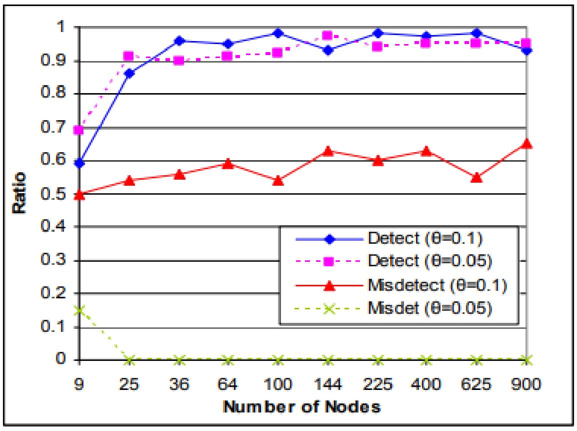


Fig system scalability

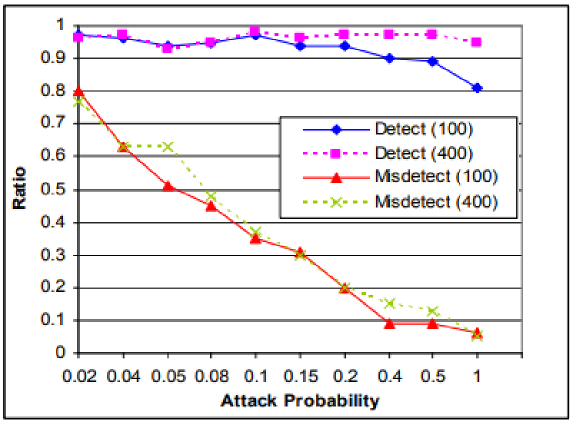


Fig Detection Accuracy vs. Compromise Probability

CONCLUSION

This manuscript presents a completely dispersed calculation permitting every hub of a DTN to appraise the status of its own sensors utilizing LODT performed during the gathering of hubs. The DFD calculation is examined considering a Markov model of the advancement of the extent of hubs with a given confidence in their status. This model is then used to determine an arrangement of customary differential conditions approximating the development of the extents of the hubs in various states. The presence and uniqueness of balance is talked about. Strangely, the extents at the balance follow a binomial circulation. The approximations of these extents of hubs at balance give knowledge to appropriately pick the choice boundary of the DFD calculation. In the recreations, a bounce movement model, a Brownian movement model, just as information bases containing hints of between contact time moments are thought of. The outcomes show a decent match with hypothesis. The intermingling velocity of the DFD calculation relies upon the between contact rate and on the extent of hubs with deficient sensors p1. In any case, p1 has not a huge effect on the non identification and bogus caution rates at harmony, indicating the strength of the methodology additionally if there should be an occurrence of an enormous number of blemished hubs. The effect of the presence of getting rowdy hubs has additionally been thought of, indicating the vigor of the proposed DFD calculation.

REFERENCE

[1] M. J. Khabbaz, C. M. Assi, and W. F. Fawaz, “Disruption- tolerant networking: A comprehensive survey on recent developments and persisting challenges,” IEEE Commun. Surveys Tuts., vol. 14,

no. 2, pp. 607–640, Apr.–Jun. 2012.

[2] P. R. Pereira, A. Casaca, J. J. Rodrigues, V. N. Soares, J. Triay, and C. Cervell_o-Pastor, "From delay-tolerant networks to vehicular delay-tolerant networks," IEEE Commun. Surveys Tuts., vol. 14, no. 4, pp. 1166–1182, Oct.–Dec. 2012.

[3] K. Wei, M. Dong, J. Weng, G. Shi, K. Ota, and K. Xu, "Congestionaware message forwarding in delay tolerant networks: A community perspective," Concurrency Comput.: Practice Experience, vol. 27, no. 18, pp. 5722–5734, 2015.

[4] P. Hui, J. Crowcroft, and E. Yoneki, "BUBBLE rap: Social-based forwarding in delay-tolerant networks," IEEE Trans. Mobile Comput., vol. 10, no. 11, pp. 1576–1589, Nov. 2011.

[5] V. N. Soares, J. J. Rodrigues, and F. Farahmand, "GeoSpray: A geographic routing protocol for vehicular delay-tolerant networks," Inf. Fusion, vol. 15, pp. 102–113, 2014.

[6] H. Zhu, S. Du, Z. Gao, M. Dong, and Z. Cao, "A probabilistic misbehavior detection scheme toward efficient trust establishment in delay-tolerant networks," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 1, pp. 22–32, Jan. 2014.

[7] L. Galluccio, B. Lorenzo, and S. Glisic, "Sociality-aided new adaptive infection recovery schemes for multicast DTNs," IEEE Trans. Veh. Tech., vol. 65, no. 5, pp. 3360– 3376, May 2016.

M. Panda, A. Ali, T. Chahed, and E. Altman, "Tracking message spread in mobile delay tolerant networks," IEEE Trans. Mobile Comput., vol. 14, no. 8, pp. 1737–1750, Aug. 2015

[8] W. Li, F. Bassi, D. Dardari, M. Kieffer, and G. Pasolini, "Defective sensor identification for WSNs involving generic local outlier detection tests," IEEE Trans. Signal Inf. Process. Over Netw., vol. 2, no. 1, pp. 29–48, Mar. 2016.

[9] J. Chen, S. Kher, and A. Somani, "Distributed fault detection of wireless sensor networks," in Proc. Workshop Depend. Issues Wireless Ad Hoc Netw. Sensor Netw., 2006, pp. 65–72.

[10] J.-L. Gao, Y.-J. Xu, and X.-W. Li, "Weighted-median based distributed fault detection for wireless sensor networks," J. Softw., vol. 18, no. 5, pp. 1208–1217, 2007.

[11] S. Ji, S.-F. Yuan, T.-H. Ma, and C. Tan, "Distributed fault detection for wireless sensor based on weighted average," in Proc. 2nd Int. Conf. Netw. Secur.Wireless Commun. Trusted Comput., 2010, pp. 57–60.

[12] M. Panda and P. Khilar, "Distributed self fault diagnosis algorithm for large scale wireless sensor networks using modified three sigma edit test," Ad Hoc Netw., vol. 25, pp. 170–184, 2015.

[13] Y. Zhang, N. Meratnia, and P. Havinga, "Outlier detection techniques for wireless sensor networks: A survey," IEEE Commun. Surveys Tuts., vol. 12, no. 2, pp. 159–170, Apr.–Jun. 2010.

[14] A. Mahapatro and P. M. Khilar, "Fault diagnosis in wireless sensor networks: A survey," IEEE Commun. Surveys Tuts., vol. 15, no. 4, pp. 2000–2026, Oct.– Dec. 2013.

[15] H. Dong, Z. Wang, S. X. Ding, and H. Gao, "A survey on distributed filtering and fault detection for sensor networks," Math. Problems Eng., vol. 2014, 2014, Art. no.
858624.

[16] E. F. Nakamura, A. A. Loureiro, and A. C. Frery, "Information fusion for wireless sensor networks: Methods, models, and classifications," ACM Comput. Surveys, vol. 39, no. 3, 2007, Art. no. 9.

[17] A. Chiuso, F. Fagnani, L. Schenato, and S. Zampieri, "Gossip algorithms for simultaneous distributed estimation and classification in sensor networks," IEEE J. Sel. Topics Signal Process., vol. 5, no. 4, pp. 691–706, Aug. 2011

[18] F. Fagnani, S. M. Fosson, and C. Ravazzi, "A distributed classification/ estimation algorithm for sensor networks," SIAM J. Control Optimization, vol. 52, no. 1, pp. 189–218, 2014.

[19] F. Fagnani, S. M. Fosson, and C. Ravazzi, "Consensus- like algorithms for estimation of gaussian mixtures over large scale networks," Math. Models Methods Appl. Sci., vol. 24, no. 2, pp. 381–404, 2014.