International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 5 Issue 3 May 2015
International Manuscript ID : 2249054XV5I3052015-20

EFFECTIVE HYBRID ALGORITHM FOR SECURITY AND PERFORMANCE IN WIRELESS SENSOR NETWORKS

Dr. Amit Sharma
Assistant Professor
School of Information Technology,
Apeejay Insitute of Management Technical Campus,
Jalandhar, Punjab, India

ABSTRACT

WSN or (Wireless Sensor Networks) are vulnerable to multiple channel attacks and attacks from the sources.WSN attacks include, Vampire Attacks, Sybil Attacks, Wormhole Attacks, SinkHole Attacks DDoS Attacks, etc. Sniffers and crackers can exploit the security vulnerabilities and loopholes to intrude and get access to multiple services available at the prospect. This research is based on development of an effective algorithmic approach to ensure higher integrity and better security in WSN by which the net efficiency and performance can be improved against the oncoming and new threats and security issues. In this paper an algorithm having a hybrid approach is developed and implemented. Using the algo the effective work performs better in terms of integrity, security and net throughput of the wireless network.

INTRODUCTION

Wireless communication is the exchange of data and services between two hosts and networks which are not effectively joined by the physical wires and cables.

Radio is the most widely recognized wireless innovation. Radio waves spectrum can be of short range , for example, a few metres for television to the thousands of kilometers for space radio interchanges. It includes all sorts of versatile,compact and settled applications,

including, cell phones, two-way radios ,PDAs, and WSA (wireless systems administration). Radio wireless communication includes carport entryway openers, GPS units, wireless, earphones, and headsets, cordless phones, PC mice, radio collectors, and satellite TV consoles.

Wireless operations eg in licence administration is unfeasable for eg to execute with the physical connections or cables.These operations are used by the IT industry to connect to ITF(information transfer frameworks). ITF includes remote controls, radio transmitters etc and utilize radio waves, acoustic vitality to exchange packets and communication without the utilization of wires thus communicated via short as well as largely separated areas.

To some degree less basic techniques for accomplishing wireless interchanges incorporate the utilization of other electromagnetic wireless advancements, for example, light, attractive, or electric fields or the utilization of sound.

WSA (Wireless systems administration) is used to address numerous network and communication issues. Portable PC clients are associated by WSA who make frequent trips from area to area. Another use is uniting versatile systems by means of satellite. A wireless transmission is used to network a LAN that must frequently change connected areas.

The circumstances that legitimize the effective utilization of wireless administration:

- In reinforcement communications interface if there is an occurrence of ordinary system disappointment,
- Compass a separation past the capacities of run of the mill cabling,
- Remotely associate portable clients or systems.
- Overcome circumstances where ordinary cabling is troublesome or monetarily illogical, or
- Connection compact or impermanent workstations

Designers need to think of some as parameters including Wireless RF innovation for better creating wireless systems:

- Sub-GHz versus 2.4 GHz recurrence patterns
- Working reach and battery life
- Affectability and data rate
- System topology and node knowledge
- Applications including point-to-point communication, point-to-multipoint communication,cell systems, TV , Wi-Fi innovation and different wireless systems..

A WSN (wireless sensor system) (some of the time called (WSAN) a wireless sensor and performer network) are spatially disseminated self-governing sensors to screen physical or ecological conditions, for eg, temperature, sound, weight, and so forth and to helpfully go their data through the system to a fundamental area.

The more cutting edge networked systems are bi-directional, empowering control of sensor movement. The advancement of wireless sensor systems was propelled by military applications, for eg, war zone observation; today such systems are utilized as a part of numerous mechanical and shopper applications, for eg, modern procedure checking and control, machine wellbeing checking, etc.

The WSN is assembled of "nodes" – from a couple to a few hundreds or even thousands, where every node is associated with one (or some of the time a few) sensors. Each such sensor system node has regularly a few sections: a radio handset with an inner reception apparatus or association with an outer receiving wire, a microcontroller, an electronic circuit for interfacing with the sensors and a vitality source, more often than not a battery or an inserted type of vitality reaping.

A sensor node may shift in size from that of a shoebox down to the extent of a grain of dust, albeit working "bits" of certifiable tiny measurements have yet to be made. The expense of sensor nodes is comparably variable, extending from a couple to several dollars, contingent upon the many-sided quality of the individual sensor nodes. Size and expense limitations on sensor nodes bring about relating imperatives on assets, for example, vitality, memory, computational pace and communications data transfer capacity. The topology of the WSNs

can fluctuate from a basic star system to a progressed multi-bounce wireless lattice system. The engendering strategy between the bounces of the system can be directing or flooding.

In telecommunications, wireless sensor systems are a dynamic exploration zone with various workshops and meetings orchestrated every year, for instance IPSN, SenSys, and EWS

LITERATURE REVIEW

To propose and defend the proposed research, a number of international journals and conference papers are investigated. Following are the extracts from the key journals and conferences.

[1] In this paper, the performance of WSN is improved by analyzing and monitoring of different attacks. The WiMax Network is localized for the higher integrity and security. The results in the paper are giving better results with the proposed solution.

[2] In wireless administered systems, a client may effectively utilize the wireless vitality exchanged from a vitality hotspot for its data transmission. In any case, because of telecast nature of wireless vitality exchange (e.g., RF vitality), a pernicious node (i.e., an assailant) can likewise block the vitality and utilization it to perform an assault by sticking the data transmission of the client. This work thinks about, for example, a sticking assault where the client and aggressor are mindful of one another. The work details a diversion theoretic model to investigate the vitality solicitation and data transmission arrangement of the client and the assault strategy of the assailant when the client and the aggressor both need to augment their own prizes. This paper utilizes an iterative calculation composed in view of the best reaction motion to acquire the arrangement characterized as far as the compelled Nash harmony. The numerical results indicate the union of the proposed calculation, as well as the ideal prize of the client under diverse vitality cost limitations.

[3] Wireless sensor systems are defenseless against a few assaults, one of them being the dark gap assault. A dark gap is a noxious node that pulls in all the movement in the system by

publicizing that it has the most limited way in the system. When it gets the parcel from different nodes, it drops every one of the bundles creating loss of discriminating data. In this paper we propose an unwavering quality examination system. The proposed unwavering quality investigation plan defeats the weaknesses of existing agreeable dark opening assault utilizing AODV steering convention. When there is a way accessible for steering, its unwavering quality is checked utilizing t he proposed plan. The proposed unwavering quality investigation plan helps in accomplishing most extreme dependability by minimizing the changing and vulnerable nature of the associated networked framework. The unchanging quality examination and utilizing the proposed plan will make the way secure enough to minimize the parcel misfortune, end - to - end delay and the vitality use of the system and also expand the system lifetime consequently

[4] Wireless sensor systems are liable to assaults, for example, node catch and cloning, where an assailant physically catches sensor nodes, repeats the nodes, which are conveyed into the system, and continues to assume control over the system. In this paper, the work create models for such an assault when there are numerous assailants in a system, and detail multi-player amusements to demonstrate the noncooperative key conduct between the aggressors and the system. This paper consider two cases: a static situation where the aggressors' node catch rates are time-invariant and the system's clone identification/renouncement rate is a straight capacity of the state, and a dynamic situation where the rates are general elements of time. We describe Nash balance answers for both cases and determine harmony systems for the players. In the static case, we concentrate on both the single-aggressor and the multi-assailant amusements inside of an improvement structure, give conditions to the presence of Nash equilibria and describe them in shut structures. In the dynamic case, the work concentrate on the basic multi-individual differential diversion under an open-circle data structure and give an arrangement of conditions to describe the open-circle Nash balance. This paper demonstrates the proportionality of the Nash harmony for the multi-individual diversion to the seat point balance between the system and the aggressors as a group. This work shows the outcomes with numerical cases.

[5] A Wireless Mesh Network (WMN) is a promising method for giving ease broadband Internet access. The basic steering convention innocently accept that every one of the nodes in the system are non-malevolent. The open building design of WMN, multi-bounce nature of communication, distinctive administration styles, and wireless communi-cation clears approach to noxious assailants. The aggressors can endeavor shrouded provisos in the multipath lattice steering convention to have a suction assault called the blackhole assault. The aggressor can misrepresent directing measurements, for example, the most limited transmission time to achieve any destination and consequently suck the system movement. We propose a novel system by utilizing versatile honeypot operators that use their topological learning and identify such spurious course notices. They are conveyed as wandering programming operators that visit the system and bait assailants by sending course ask for notices. We gather profitable data on assailant's strategy from the interruption logs accumulated at a given honeypot. This work at long last assess the viability of the proposed structural engineering utilizing reproduction as a part of ns-2.

[6] Malware assaults constitute a genuine security chance that debilitates to back off the substantial scale multiplication of wireless applications. As an initial move toward impeding this security danger, we look to measure the greatest harm exacted on the framework because of such episodes and distinguish the most horrible assaults. This work speak to the engendering of malware in a battery-obliged versatile wireless system by a pandemic model in which the worm can alterably control the rate at which it executes the contaminated node furthermore the transmission ranges and/or the media examining rates. At every snippet of time, the worm at every node confronts the accompanying tradeoffs: 1) utilizing bigger transmission extents and media examining rates to quicken its spread at the expense of debilitating the battery and in this manner decreasing the general disease proliferation rate over the long haul; or 2) killing the node to cause a vast cost on the system, however to the detriment of losing the possibility of tainting more helpless nodes at later times. We numerically detail the choice issues and use Pontryagin Maximum Principle from ideal control hypothesis to measure the harm that the malware can exact on the system by sending ideal choice standards. Next, we build up basic properties of the ideal method of the assailant

after some time. In particular, we demonstrate that it is ideal for the aggressor to concede killing of the infective nodes in the proliferation stage until coming to a certain time and after that begin the butcher with greatest exertion. We additionally demonstrate that in the ideal assault strategy, the battery assets are utilized by diminishing capacity of time, i.e., most forcefully amid the introductory period of the episode. At long last, our numerical examinations uncover a system for distinguishing keen resistance procedures that can restrict the harm by fittingly selecting system parameters.

[7] Wireless sensor system is a much circulated system of little lightweight wireless sensor nodes, sent in huge numbers to screen the earth or framework. These sensor systems have constraints of framework assets like battery force, radio extent and processing capacity. Low preparing force and wireless integration make such systems defenseless against different assaults like sink opening, dark gap, Sybil assaults, specific sending, worm gap, hi surge and so forth. Among these welcome surge assault is a critical attack on the system layer, in which a foe, which is not a lawful node in the system, can surge hi solicitation to any true blue node utilizing high transmission power and break the security of WSNs. The present answers for this kind of assault are basically cryptographic, which experience the ill effects of substantial computational many-sided quality. Thus these are less suitable as far as memory and battery power. In this paper a system has been proposed to distinguish and avert hi surge assault utilizing sign quality of got Hello messages. Nodes have been delegated companion and outsider in light of the sign quality of Hello messages sent by them. Nodes named more abnormal are further accepted by sending a basic test parcel; if the answer of test bundle returns a predefined time then it is dealt with as legitimate else it is dealt with as malevolent. The calculation is executed in ns - 2 by altering the AODV - directing convention. The execution of calculation has been tried under diverse system situations. The recreation results s how enhanced execution of the new calculation as far as number of parcel conveyance proportion as contrast with AODV with hi surge assault.

[8] A wireless sensor system comprises of numerous sensor nodes which are sent to screen physical or natural conditions and to pass the gathered data to a base station. In spite of the

fact that wireless sensor system is subjected to have real applications in every one of the zones, it additionally has numerous security dangers a d assaults. Among all dangers, for example, sinkhole, wormhole, particular sending, refusal of administration and node replication, Sybil assault is a noteworthy assault where a sing le node has various characters. At the point when a Sybil node go about as a sender, it can s end false data to its neighbors. When it goes about as collector, it can get the data which is initially bound for a honest to goodness node. The current arrangements expend more vitality. So a vitality proficient calculation named Sybilsecure is proposed. Trial results demonstrate that Sybilsecure expends less vitality than existing guard components.

PROPOSED WORK AND IMPLEMENTATION

The classical works of wireless sensor networks are having number of threats and vulnerability issues. In the proposed work is having the approach of multi layered security to provide the higher efficiency, accuracy and lesser cost factor for any kind of scenarios. The proposed work can be implemented for any kind of wireless network with mobility and any number of nodes can be integrated therein.

- *The proposed work integrates the simulated annealing with the hybrid approach of the security based hash algorithms.*
- *Using proposed approach, the current or greedy solution is compared with the earlier results and solutions.*
    - *Let* $s = s_0$
    - *For* $k = 0$ *through* k_{max} *:*
        - $T \leftarrow$ *temperature (SA Variable)* (k / k_{max})
        - *Pick a random neighbour,* $s_{new} \leftarrow$ *neighbour(s)*
        - *If* $P(E(s), E(s_{new}), T) >$ *random(0, 1), move to the new state:*
            - $s \leftarrow s_{new}$
    - *Output: the final state s*
- *In this case, the solution is the security aspect and cost factor.*

International Journal of Computing and Corporate Research
ISSN (Online) : 2249-054X
Volume 5 Issue 3 May 2015
International Manuscript ID : 2249054XV5I3052015-20

- *The dynamic own and novel encryption keys are matched at assorted phases to enrich and strengthen the security.*
- *The integration of own developed novel hash algorithm is done to make the keys secured*
- *The current solution is accepted if the security factor and cost factors are optimized from the previous solutions.*

Table 1 - Simulation Based Comparison of Classical and Proposed Approach in terms of Security

Wireless Sensor Nodes	Classical Approach	Proposed Approach
5	30	48
10	55	69
15	47	60
20	40	59
25	70	89

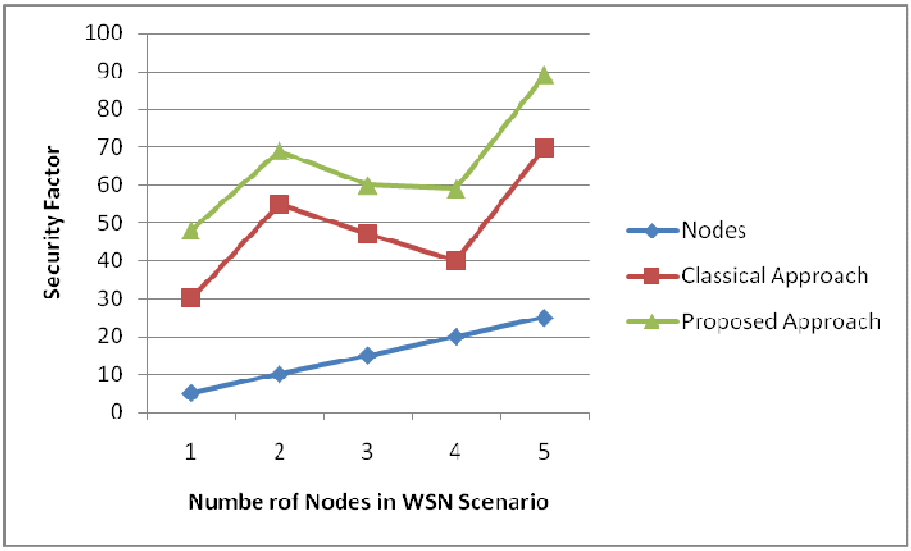

Figure 1 - Line Graph Comparison of Classical and Proposed Approach in terms of Security

Table 2 - Simulation Based Comparison of Classical and Proposed Approach in terms of Cost

Wireless Sensor Nodes	Classical Approach	Proposed Approach
5	45	30
10	59	42

15	68	55
20	72	64
25	80	70

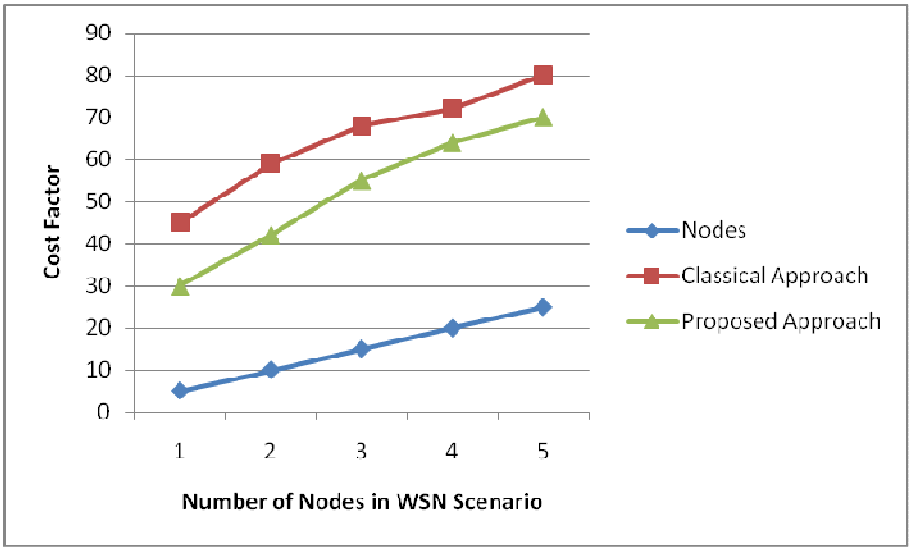

Figure 2 – Line Graph Comparison of Classical and Proposed Approach in terms of Cost

From the results and implementation, it is evident that the cost factor and security factor is improved and optimization in the proposed approach. The proposed algorithm is having higher integrity and security for any number of nodes.

CONCLUSION

The proposed research work is associated with the development of an effective algorithm for higher security and integrity in the wireless sensor networks. Number of other research domains in WSN includes Routing, Scheduling, Energy Optimization, High Performance Computing and many others. The major reason behind choosing security is that this domain is unending and having lots of scope in research and development. A no. of research algo are developed so far for avoidance of attacks and malicious code identification, still there is huge scope of work. In this proposed and implemented work, the performance of the network is improved by integrating the aspect that the malicious node is not able to find and use the actual key generated at the source node. The key is merged with a set of non genuine keys so that the attackers are disguised. By this method, the security is enhanced. For implementation

and simulation of the existing and proposed work, the simulation techniques are used. Different parameters and aspects including the probability of finding out and investigation of the successful and failure attempts are analysis. Using simulation and modelling technique, we have obtained effective results in assorted dimensions as compared to the base algorithmic approach.

REFERENCES

[1] Niyato, D., Wang, P., Kim, D. I., Han, Z., & Xiao, L. (2015). Game Theoretic Modeling of Jamming Attack in Wireless Powered Networks. *Proc. of IEEE ICC, London, UK*.

[2] Khouzani, M. H. R., Sarkar, S., & Altman, E. (2012). Maximum damage malware attack in mobile wireless networks. *Networking, IEEE/ACM Transactions on*, *20*(5), 1347-1360.

[3] Singh, V. P., Ukey, A. S. A., & Jain, S. (2013). Signal strength based hello flood attack detection and prevention in wireless sensor networks. *International Journal of Computer Applications (0975–8887)*.

[4] Umamaheswari, S., & Mahalakshmi, R. (2015). Dynamic Network Event Analysis for Distributed Attack Detection in Wireless Sensor Networks. *Sensor Letters*, *13*(1), 64-71.

[5] Prathapani, A., Santhanam, L., & Agrawal, D. P. (2013). Detection of blackhole attack in a Wireless Mesh Network using intelligent honeypot agents. *The Journal of Supercomputing*, *64*(3), 777-804.

[6] Virmani, D., Soni, A., & Batra, N. (2014). Reliability Analysis to overcome Black Hole Attack in Wireless Sensor Network. *arXiv preprint arXiv:1401.2540*.

[7] Karuppiah, M. A. B., & Prakash, A. R. (2014). Sybilsecure: An Energy Efficient Sybil Attack Detection Technique In Wireless Sensor Network. *International Journal of Information*, *4*(3).