International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

Security Aware Reliability Model for WBANs

Vinay Pathak, Karan Singh

Abstract*: Today we are living in the midst of technological revolutionary world where use and misuse of technology is very often and increasing day by day. Every day due to advent of technological development new challenges are being faced by all technological fraternity. Types of new attacks are taking place on cyber world to prevail physical attacks as dependency increases on cyber world. Today we need to investigate security of reliability to keep our self-securefrom external attack and need to rethink about old definition of reliability of any cyber world. In this we emphasis on the wireless body area network (WBANs) because of or reason its usability and nature. The most basic and crucial parameter of WBANs is reliability. In this type of investigation, the innovator examine the reliability quality of WBANs dependent on the system entire lifetime, and infer a general equation of dependability as far as the quantity of small notes which have capability to sense and gathering trademark parameter (GCP). Bottom and top limits of the reliability quality are must be f determined for self-assertive WBANs by analysis of their group characteristic parameter (GCP).

***Index Terms*: Group Characteristic Parameter (GCP), Reliability, Security Constant, Wireless body area network.**

I. INTRODUCTION

Reliability is a most critical insecure parameter WBANs because security of reliability is not accessed usually. In view, the monotonicity belongings of reliability quality, is a calculation by utilizing normal GCP is exhibited to figure the base and most extreme number of small nodes which have capability to sense for a predefined system, and we calculate the ideal number of small nodes which have capability to sense for a given reliability quality. New security constant will be needed to minimize the life loss with reliability due to more number of attacks are reported or notice every day.

The execution of dependability is assessed through numerical outcomes. Current advancement in wearable and embedded wellbeing checking advances can possibly change the eventual fate of social insurance benefits by empowering universal observing of patients. A run of the mill wellbeing observing framework comprises of a system of wearable or embedded sensors that continually screen physiological parameters. Gathered information is transferred utilizing existing remote correspondence conventions to a base station for extra handling. This article furnishes scientists with data to look at the current low-control correspondence innovations that can possibly bolster the fast advancement and organization of WBANs frameworks, and for the most part centers around remote observing of elderly or constantly sick patients in private situations. WBANs have been a potential road for future digitized social insurance frameworks. WBANs have one of a kind difficulties and highlights contrasted with different remote sensor systems. Notwithstanding battery control utilization, the weakness and the unpredicted channel conduct make channel get to a major issue. Remote body region systems (WBANs) contain some low-control, scaled down, obtrusive or uninstructive, small notes which have capability to sense with remote correspondence which work in the closeness of a person body. All these small notes which have capability to sense are put around the body, or, in other word not the similar as remote sensor systems (WSNs). WSN mostly utilizes radio correspondence mode rather than one to one mode. In differentiate, WBANs concentrates much more on the reliability quality information in light of the fact that the remote correspondence on or around a person body has much interest in correspondence most significant feature. Additionally, the transfer of signal from one point to another point and its control in WBANs is clearly less than as it in WSN on the grounds that it is limited by not pre fixed and changeable as per demand condition around the person body. Contrasting and WSNs, we have to guarantee the continuous, security, what's more, exactness of the data. Energizing worldwide market openings are opening rapidly for new electronic items that can serve and empower the rising shrewd society. Renesas Electronics Corporation is proceeding to design and create propelled semiconductor answers for this zone, particularly gadgets for actualizing remote sensor organizes, the subject of our two-section EDGE arrangement. This second story looks at Body Area Networks, clarifies electric-field correspondence, and features some encouraging WBANs applications.

WBAN is a short-extend remote system contained gadgets situated in, on, and around the body. It gives information correspondence over short separations, constrained to scopes of only a couple of meters. This new, inalienably close to home sort of system utilizes wearable and embedded electronic circuits. It actualizes exceedingly valuable capacities and abilities in advantageous, subtle setups that work at low power and convey superlative security. Generally couple of items and applications dependent on WBANs innovation exist today. In any case, that circumstance isn't probably going to keep going for long. Renesas foresees colossal development from creative usage and refinements. It is normal that WBANs items will quickly wind up prominent and deals will soar, similarly as has been the situation for some sorts of individual electronic gadgets. Radio communication mode is used by WSN rather than point to point communication.

Manuscript published on 30 June 2019.
***** Correspondence Author (s)
Vinay Pathak*, Department of Computer Science, School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India.
Karan Singh, Department of Computer Science, School of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi, India.

In differentiate WBANs concentrates more on the reliability quality of the information in light of the fact that the remote correspondence around person body has very much interest for correspondence quality. Also, control of the transmission in WBANs is clearly showing not much than it in WSN in light of the fact that it is confined by a not fixed feature condition around the person body. Contrasting and WSNs, we should have to give the guarantee of continuous, security, and what's more, exactness of the data.

II. LITERATURE REVIEW

WBANs has been come too noticed to bolster best usable app in social insurance, wellness along with individual excitement [1]. That means to disentangle and enhance the speed, exactness, and reliability quality of respective or correspondence of sensors [2]. Reliability quality of respective is requested for building up a number of utilizations in a few fields [3]. For expanding dependability, a novel demonstrating and investigation of hub practices in WBANs is introduced within the sight of multi-type is appointments [4]. In WBANs, the radio-frequency (RF) signals transmitted from the around-body or in-body bio-sensors to access points (AP) feels in a not predefined channel which dynamic in nature. Further the basic nature of small node cable to sense (e.g., low power, low expenditure, and small piece rate) of the short-range wireless communication networks require highly bendable and reliable design plan and protocols at the time of designing the scheme for the transmission of data. Furthermore, the efficiency of e-wellbeing wireless device is directly affected by the complex structure or complex nature of human body [5]. Because of unreliable data transfer has very negative and dangerous impacts on healthcare, and the consequent of compromise with reliability parameter can put the patients 'life at risk due to such sporadic nature of attacks or any other nature of attack. (*like* DoS *etc*) [6, 7], Due to that proper attention needs to perk-up or gear up the quality and reliability of WBANs. In paper, we delineate and investigate the different-different features which are highly affecting the reliability parameter of any network and its lifetime. Therefore, Achieving the desirable secure lifetime of network with desired reliability standard becomes a highly imperative or key issue. Numerous vitality effective conventions have been invented and proposed by researched to boost or scale-up the secure reliable life of WBANs system [5, 6]. A novel connection adjustment instrument to amplify vitality productivity in IEEE 802.15.6 motivation radio ultra-wide WBANs (IR-UWB) is described in [9].

In any case, there are not many references alluded to the investigation of the system reliability quality in WBANs. The reason for this paper is to investigate the execution of system dependability dependent on different–different factor of WBANs. We initially infer a common or all-purpose recipe for computing the dependability of the WBANs dependent on system lifetime. This paper is sorted out as pursues. Area 2 introduces the organize model and lifetime definition of WBANs. Area 3 infers a general reliability quality equation. In section 4, a calculation is proposed to enhance the quality of sensors. Numerical outcomes for the same are appeared in Area 5. At long last, Section 6 closes with the conclusion and possible. Social insurance applications have pulled in analysts' consideration as a result of the increasingly maturing populace inclined to age-related maladies and could regularly profit by constant checking of physiological signs [2]. The utilization of WBANs may give power to ubiquitous human services and could lead to proactive, and even remote, demonstrative of ailments in a beginning time. Also, WBANs may include an actuator, which depends on estimations and settings can naturally discharge solution. A precedent being an actuator on the way to deliver insulin to a human patient suffering with diabetes by decent or apt conditions. Furthermore, WBANs give wellbeing observing without meddling the patient's or persons ordinary exercises.

For ongoing applications where the parental figure needs to get data about the concern one wellbeing on a consistent premise, the WBANs ought to give, amongst other qualities, solid correspondences with the purpose of are generally uncaring to connection or hub disappointments [3]. Be that as it may, quiet portability expands the likelihood of bundle misfortune, and it is favoured that the bundle blunder rate ought to be kept not exactly 1% [4]. In addition, the WBANs must broadcast or convoy at near to the ground power to make sure the patients against unsafe wellbeing impacts related with the radiofrequency (RF) outflows. Accordingly, the particular retention rate (SAR) ought to be small [5]. SAR is the rate at which the RF vitality is consumed by a volume of body or mass. Because of above said, confinement on the particular ingestion rate, it isn't conceivable to expand the transmission control past a certain level to punch the broadcast loss of the parcels. For achieving the objectivity a method based on link adaptation which based on frame error rate for their estimation is proposed [2, 9] for OFDMUWB which have many WBANs and referred as multi WBANs.

Specifically, remote indispensable signs observing is a territory of present day medicinal services that is becoming quick [2, 8]. Sensium is a trademark of Toumaz Technology Ltd, UK. Indispensable signs checking utilizing WSNs organize innovations have beforehand been portrayed, however these frameworks are ordinarily massive and control hungry and depend on MAC conventions, for example, Bluetooth and 802.11 which are wasteful for such or like this or above said WBANs applications [3][4][5][6,8]. More broad WSN MAC conventions, in fact, it's become the focal point of escalated research [6], [7,8], [9], [10], are additionally not appropriate to these particular biomedical WBASN applications either.

In determining this MAC Protocol, the accompanying characteristics can be derived about the WBANs sensor arranges.

- All node sensor hubs of WBANs are connected to the human or patient body.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

- Checked information has the very low recurrence.
- Instantly is no process to change the system or there is in the system no process to make change in system instantly. (Can be induced from 2).

Sensors screen a scope of fundamental signs which are commonly at a low information rate (<1kB) e.g., Temperature, weight or pulse perusing. Anyway some higher information rate applications should likewise be provided food for, for example, gushing a record or display of a person's heartbeat produced by electrocardiogram (ECG).

The hubs are scaled down; battery fueled and need to run in a perfect world for a considerable length of time from low limit batteries, for example, adaptable printed battery advancements or miniature coin cells.

- Resource constrained is a critical parameter for small sensor nodes.
- To process the data, data are forwarded from small wireless sensor node to a central master node. Central node has more resource significantly as compared to another wireless node.

The utilization of WBANs innovation requires redress conveyance of the indispensable physiological indications of the patient alongside the vitality administration in power-compelled devices.

The main objectivity to use Modern wireless implant technology needs accurate delivery or parcel of patient by managing the energy in most prone to power constrained devices or in digitized e wellbeing devices. WBANs sup-port an expansive scope of therapeutic/non-restorative applications in home/human services, medication, sports, and so forth. Of intrigue is the utilization of WBANs for the consistent remote checking of the fundamental physiological indications of patients, paying little mind to the constraints on their areas and exercises. The dependability of WBANs is the capacity of the system keeping associated even while experiencing disappointments and pernicious assaults. Vindictive clients may endeavor to get the patient data, for example, indispensable sign and persistent ID, utilizing security assaults, for example, wormholes and spoofing. WBANs hubs ought to be ensured from previously mentioned disappointments and pernicious assaults.

A reproduction or simulation or experiment in virtual environment has been done for demonstration the effect of bad conduct hubs on system reliability quality. This is accepted to be the first endeavor to display the misconduct hubs in WBANs which is extremely helpful to break down the reliability quality of the WBANs. Additionally investigate work may incorporate performing relationship contemplates between genuine test-bed estimations and reproduction.

Framework builds on R& D ventures went for creating WBANs and remote sensor organizes regularly confront configuration challenges in two regions that affect the reliability quality of the system correspondence: flag shortcoming and clamour impedance. Fruitful plan approaches must utilize semiconductor gadgets that guarantee stable correspondence. Discontinuous network can't be permitted; the information stream ought to be persistent.

One framework outline issue in such manner is that the flag at the collector in WBANs that applies electric-field correspondence is especially powerless, in light of the fact that a significant part of the actuated charge spills out through the transmitter and ground. As needs be, there is a need to create more grounded getting innovation; i.e., chips that can dependably identify low-level signs. Our semiconductor engineers are finding imaginative approaches to limit flag misfortune and amplify recipient affectability and selectivity, to boost information exchange reliability quality.

The developing expense of human services and the maturing populace in created nations have presented awesome challenges for governments, human services suppliers and medicinal services industry. There is incredible enthusiasm for utilizing rising remote advancements to help remote patient checking in an inconspicuous, solid and cost viable way in this way giving customized supportable administrations to patients.

Access method Bearer Sense Multiple Access (CSMA) also, Time Division Multiple Access (TDMA) is well known medium access procedures utilized in WBANs. In a CSMA based convention, hub will initially detect the bearer *i.e.* tunes in to the medium. In the event that no action is seen, the hub will begin its transmission. Something else it will begin a back-off technique where it will probabilistically sit tight for a given time. The fundamental thought behind TDMA is to control access to a common medium by separating time in little fragments, called spaces. Hubs wishing access to the medium are appointed at least one of these openings.

Despite the fact that CDMA is an elective getting to system in WWBANs, TDMA is the most favored one as it gives opening reservation to hubs giving higher dependability than CDMA. In addition defer ensures are stricter in CDMA than in TDMA. The correspondence in WWBANs is a type of numerous to one correspondence where all movement wind up at a solitary point in the system. In WWBANs, the activity from sink to the hubs ought not to be barred in any case, the vast majority of the movement considered to spill out of hubs to the sink. Control activity most likely spill out of sink to the hubs however fundamentally littler than the measure of information movement from hubs to the sink. As WBANs thought to be an associated system, hubs can either make an immediate association with the sink or it can depend on different hubs to reach.

To disentangle the examination and to bring high vitality effectiveness the vast majority of the exploration works accept symmetric connections and multi- bounce topologies in WBANs, in spite of the fact that this may not be the situation truly.

The accompanying shows some primary contrasts between WBANs and Remote Sensors.

There are no repetitive gadgets in WBANs in spite of WSNs. All hubs in the system must be profoundly strong, solid, and precise. The lost data from one hub frequently can't be recouped by other hubs.

In light of the unique highlights of the earth in which the WBANs works (human body) the information misfortune is more critical.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

The signs of the sensors, exceptionally the embedded ones, are extensively weakened in light of the fact that the waves happens in or around and tremendously lossy medium.

Restrictive instruments might be required to guarantee the QoS and ongoing information cross examination abilities. In any case, in WSNs the information misfortune might be secured by different sensors.

The sensors which are either embedded into a tissue or connected on the surface of body must be extremely little in size to help subtle observing of the patients. In any case, in WSNs the sensor estimate is not the principle concern however littler sensors are favored. The little size of the WBANs sensors seriously influences the power assets of the gadgets. The power supply energize of the gadgets is frequently inconceivable. Along these lines, a long lifetime of the sensors is required. The sensors in WBANs are situated in or taking place on human body which is in movement because of body movement. This test for WBANs is infrequently accessible for WSNs. In this way the WBANs must be hearty against the high likely arrange topology changes. What's more, organic variety and multifaceted nature cause a more factor structure.

III. Proposed Work and Result Discussion

IEEE 802.15 task group formally define WBANs. The node of WBANs who have sensing potential work like other node usual node of network but they are responsible to collect and transmit most critical & valuable information of universe or as compare to other network. Hence we need a network which is reliable secure in the nature. Most of the case we test the 'reliability of security' but security of reliability often considered.

There are main possible scenarios as given below:

1. No attack (ideal condition)
2. Attack (on few node)
3. Secure network (Reliability &Security constant)

To improve the reliability factor in practicality we must incorporate something factor or security with reliability of network so that even reliability of network so that even reliability drop little bit in sense in the sense of sending packet or data for one point to another but transmitted data must be secure form external attack.

In the suggested model WBANs is considered the competent of following things or components.

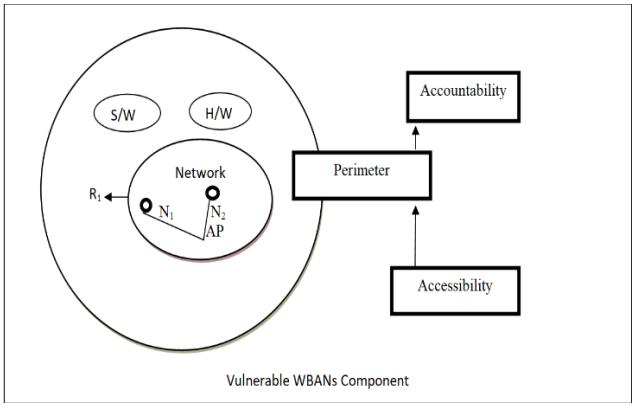

Fig: 1-Vulnerable WBANs component

In network, a group of node are used which are capable to sense the data an each group have a GCP. Any group is collection of a small – small node and network has in group. Therefore, we calculate the reliability of each component and sum of reliability of their component is overall reliability of network. Chance of probability of attack on each component is higher due to nature of information carried.

Assuming a WBANs which have AP and N and all component (SW_i, HW_i, &Ni). Numbers of small node and secure are classified in M group, each group having number of small node Sni. The reliability of any node or X^{th} node in Y^{th} group is defined by R_{xy}.

Total reliability of network WBANs is reliability of sum of each component in different scenario. To normalize the attack which is externally done by external forces we categorized or divide the group as per the severity or relevance of data. For ex. Suppose want to collect data of fever we can wear so that no life loss is our security constant. Security constant is the result of our secure algorithm.

Let's assume the intensity of attack is point two and a person having 100 degree C fever and 150 heart beat minimum then due to attack 100 degree c become 102 and 153 so we need more power full medicine so catch heart beat which result lower is again a great threat for life. So we put security constant as requirement.

$$R=R_1+R_2+R_3 \quad \text{(Reliability each Components)}\ldots (1)$$

The total reliability is represented as:

$$R(Y) = \sum_{i=1}^{m} \quad \sum_{j=1}^{n} R_{xy} \ldots (2)$$

R_{xy} is mutually independent random variable random variable with density $\lambda_i e^{-\lambda i t}$ u(t).sc means $\lambda_i e^{-\lambda i\ X}$ u(x) sets when there is no attack ideal situation there.

$$f(y) = \int \Omega \sum_{k=0}^{\infty} \frac{\delta_k\ \lambda_{m>\lambda}^{n+k} y^{k-1}}{(n+k-1)!} e^{-\lambda_{max}\ y} \quad y > 0 \qquad \ldots (3)$$

and in *Eq.* (3) define only reliability without consideration of security constant is more and less.

Cases

In case of any type of cyber-attack total reliability of data is severally degraded but reduced the threat to life.

Actual reliability (AR)= $R_1+R_{2(SW)}+R_{3(HW)}\ldots$ (4)

Then in eq.(4) R_1, $R_{2(S/W)}$& $R_{3(H/W)}$the reliability individual component then total reliability is the sum of all the reliability of each component. But in case of network which consist number of node.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

The secure reliability of network is only depends on the reliability of each node or sensor. In eq. (5) Sn_i is the number of node in network, SW_i is number of software used, HW_i is the no. of hardware component need to make network.

$$AR = R_1 \sum_{i=1}^{n} (Sn_{i=1,2..n}) + R_2 \sum_{i=1}^{sn} (SW_i) + R_3 \sum_{i=1}^{Hn} (HW_i) \dots (5)$$

Reliability probability of component or elements of network is:

$$AR_{s_{ni}} = RS_{n_{i=1}} + RS_{n_{i=2}} + \cdots + RS_{n_{i=n}} \quad \dots (6)$$

$$AR_{s_{ni}} = R(1-P)S_{n_{i=1}} + R(1-P)S_{n_{i=2}} + \cdots + R(1-P)S_{n_{i=n}} \quad \dots (7)$$

If the probability of any node is less than the desired security level, value will to be discarded.

Failure condition:

- If data given by any node reaches less as pre-defined value of that group
- A failure occurs due to non-functioning of node.
- A failure occurs due to external attack.

Then we $\lambda_i e^{-\lambda_i(t)}.SC$ to achieve accurate data as predefine SC>0.

Probability of component is either therefore workable or not but in network each node have .5 probability and addition of all probability is must meet pre-defined value then only data will be forwarded. Suppose m group have S_{ni} nodes. Then probability of

- P(m, S_{ni}) is success on all node working well
- $P(m, s_{ni})(1-P)$
- $P(m, s_{ni}) = 0$

$$f(y) = \left\{ \Omega \sum_{k=0}^{\infty} \frac{\partial_k \lambda_{max}^{n+k} y^{n+k-L}}{(n+k-1)!} e^{-\lambda_{max} y} \quad \dots (8) \right.$$

Where Ω, ∂_k and y_m are defined as

$$\Omega = \prod_{i=1}^{m} ((\lambda_i \mid \lambda_{max})^{n_i}).sc \quad \dots (9)$$

$$\partial_k = \frac{1}{k}\left(\sum_{m=1}^{k} m_{r_m}\, \partial_{k-m}\right).sc \quad \dots (10)$$

$$r_m = \sum_{i=1}^{m} n_i \left(\frac{(1-\lambda_i/\lambda_{max})^m}{m}\right).sc \quad \dots (11)$$

$$\lambda_{max} = max_{k<i<m}(\lambda_i)$$

$$k = 1,2,3 \dots n$$

$$m = 1,2,3 \dots n$$

$$\delta_0 = 1$$

Proof: Let $y_i = \sum_{y=1}^{n_i} R_{xy}$ every source in one group of independent, assuming one malicious data cannot make maliciousness in all data.

It is discarded immediately. It is a variable random in nature. The probability y_i have

$$f(y_i) = \left[\left(\lambda_i^{n_i} r_i^{n-1} \middle| (n_i - 1)!\right) e^{-\lambda}\right].sc \quad \dots (12)$$

Where $s_{ni} > 0$

$$R(y) = P(y > j) = \left(1 - \int_{-\infty}^{1} f(y) d_y\right).sc$$

$$R(y) = \begin{cases} -1, \Omega \sum_{k=0}^{\infty} \frac{\delta_k \lambda^{n+k} u^{n+k-1}}{(n+k-L)!} e^{-\lambda \max y} d_y \; y > 0 \\ 1, \quad otherwise \end{cases}$$

In the segment we will drive optimality of node of small node and optimality of each number of small in WBAN

Let's assume for 1 small node and one group then for maximum R(y)=1 id minimum number of sensor then for maximum reliability R(y)≈0is scanty constant.

If one node then probability is 0.5 and as number of node increase probability in universally proportional to success defined by

$$P = \frac{1}{2} n_1 + 1\, n_2 + 0 n_3 + 0 n_4 \dots + n_n$$

If all will give .5 SC the data is forwarded. So SC (security constant) plays as an important role to increase overall secure reliable data Transmission form one place to another.

Flow of programmatically implementation is given below.

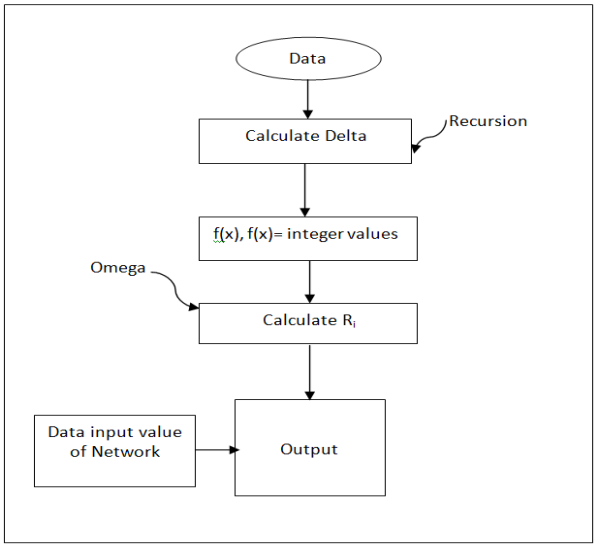

Fig: 2 Flow of Implementation

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

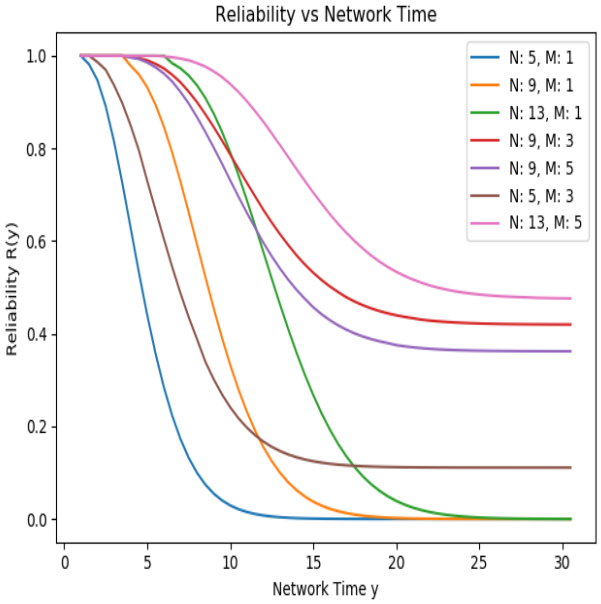

Fig: 3-without security constant reliability

Figure-3 give us the reliability factor without the consideration of security constant. Packet delivery reliability is good but how many of them is not useable due to attack is not incorporated in that whereas figure-4 give us result after inclusion of security constant and it will discard the packet as per the GCP of group.

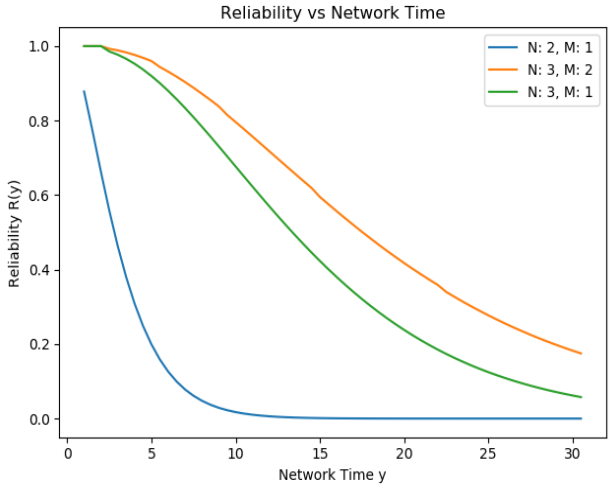

Fig: 4: Secure reliable

IV. DISCUSSION

According to the above experimental result and analysis, this section focuses on the following key-features.
In this most technological vulnerable world security is the most prominent thing. In this model by adding security constant we cater the security problem. So by the addition of security parameter this model is more reliable.

V. CONCLUSION

In this paper we will improve the overall reliability by adding the security constant in reliability absence which is very dangerous in the midst of cyber-attack world. We use world security constant and utilize same as per the severity and criticality of data to minimize the human life loss. In near future we will extend same to increase reliability of WBANs with security so that sporadic attacks can be catering effectively on cyber world or WBANs.

ACKNOWLEDGMENT

This work was carried out in network security laboratory, SC&SS, JNU, New Delhi, India sponsored by UPE-II grant.

REFERENCES

1. Patel, M., Wang, J.: 'Applications, challenges, and prospective in emerging body area networking technologies', IEEE Wirel. Commun. Mag., 2010, 17, (1), pp. 80–88
2. Movassaghi, S., Abolhasan, M., Lipman, J., et al.: 'Wireless body area networks: a survey', IEEE Commun. Surv. Tutor., 2014, 16, (3), pp. 1658– 1686
3. Cavallari, R., Martelli, F., Rosini, R., et al.: 'A survey on wireless body area networks: technologies and design challenges', IEEE Commun. Surv. Tutor., 2014, 16, (3), pp. 1635–1657
4. Wang, S., Park, J.-T.: 'Modeling and analysis of multi-type failures in wireless body area networks with semi-Markov model', IEEE Commun. Lett., 2010, 14, (1), pp. 6–8
5. Abouei, J., Brown, J.D., Plataniotis, K.N., et al.: 'Energy efficiency and reliability in wireless biomedical implant systems', IEEE Trans. Inf. Technol. Biomed., 2011, 15, (3), pp. 456–466
6. U. Varshney, S. Sneha, "Patient monitoring using ad hoc wireless networks: Reliability and power management", IEEE Commun. Mag., vol. 44, no. 4, pp. 49-55, Apr. 2006.
7. Zhang, H., Cheng, P., Shi, L.: 'Optimal denial-of-service attack scheduling with energy constraint', IEEE Trans. Autom. Control, 2015, 60, pp. 3023– 3028
8. Zhang, H., Cheng, P., Shi, L., et al.: 'Optimal DoS attack scheduling in wireless networked control system', IEEE Trans. Autom. Control, 2016, 24, pp. 843–852
9. Omeni, O., Wong, A., Burdett, A.J., et al.: 'Energy efficient medium access protocol for wireless medical body area sensor networks', IEEE Trans. Biomed. Circuits Syst., 2008, 2, (4), pp. 251–259
10. Mohammadi, M.S., Dutkiewicz, E., Zhang, Q., et al.: 'Optimal energy efficiency link adaptation in ieee 802.15. 6 ir-uwb body area networks', IEEE Commun. Lett., 2014, 18, (12), pp. 2193–2196
11. Papoulis, A., Pillai, S.U.: 'Probability, random variables and stochastic processes' (McGraw-Hill, 2002, 4th edn.)
12. Moschopoulos, P.G.: 'The distribution of the sum of independent gamma random variables', Ann. Inst. Statist. Math. A, 1985, 37, pp. 541–544
13. E. Reusens, W. Joseph, B. Latr, B. Braem, G. Vermeeren, E. Tanghe, L. Martens, I. Moerman, C. Blondia, "Characterization of on-body communication channel and energy efficient topology design for wireless body area networks", IEEE Trans. Inf. Technol. Biomed., vol. 13, no. 6, pp. 933-945, Nov. 2009.
14. R. Schmidt, T. Norgall, J. Mrsdorf, J. Bernhard, T. von der Grn, "Body area network BAN: A key infrastructure element for patient-centered medical applications", Biomed. Tech. (Berl), vol. 47, pp. 365-368, Jan. 2002.
15. J.-Y. Oh, J.-H. Kim, H.-S. Lee, J.-Y. Kim, "PSSK modulation scheme for high data rate implantable medical devices", IEEE Trans. Inf. Technol. Biomed., vol. 14, no. 3, pp. 634-640, May 2010.
16. Ding M, Chen D, Xing K, Cheng X, "Localized fault-tolerant event boundary detection in sensor networks," IEEE Infocom, 2005, pp. 902–913.
17. Ye F, Luo H, Cheng J, Lu S, and Zhang L, "A two-tier data dissemination model for large-scale wireless sensor networks," ACM Mobicom, Atlanta, GA, 2002.
18. K. Y. Yazdandoost, R. Kohno, "Body implanted medical device communications", IEICE Trans. Commun., vol. E92-B, no. 2, pp. 410-417, Feb. 2009.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

19. B. Zhen, M. Patel, S. Lee, and E. Won, "Body area network (WBANs) tech- nical requirements," IEEE 802.15.6 T echnical Requirements Document, v 4.0, 2008.
20. U. Varshney and S. Sneha, "Patient monitoring using ad hoc wireless networks: reliability and power management,"IEEE Communications Magazine , vol. 44, no. 4, pp. 49–55, April 2006.

AUTHORS PROFILE

Vinay Pathak earned the Engineering degree (Computer Science & Engineering) from Uttar Pradesh Technical University Lucknow, UP, India. He is the M.Tech. (Computer Science & Engineering) from Gautam Buddha University, UP. Mr. Vinay is currently pursuing Ph.D. (Computer Science & Engineering) from School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi, India. His primary research interest includes Network security, Cyber Secrurity, IoT, and Body Area network. He has published various papers in national and international journals or repute and conferences.

Dr. Karan Singh received the Engineering degree (Computer Science & Engineering) from Kamala Nehru Institute of Technology, Sultanpur, UP, India. He is the M.Tech. (Computer Science & Engineering) an Ph.D. (Computer Science & Engineering) from Motilal Nehru National Institute of Technology UP, India. He worked at Gautam Buddha University, UP, India. Currently, he is working with School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi. His primary research interests are in Computer network, Network security, Multicast communication, IoT, and Body Area network. He is supervisor of many researcher scholars. He is reviewer of Springer, Taylor & Francis, Elsevier Journals and IEEE Transactions. He is an Editorial Board Member of Journal of Communications and Network (CN), USA. He published 70+ research papers in refereed journals and good conferences. He organized the workshops, conference Sessions and trainings. Dr. Singh worked as General Chair of the international conference (Qshine 2013) at Gautam Buddha University, India. Recently he organized a conference ICCCS 2018 at Dronacharya College of Engineering, Gurgaon and special session in 2nd ICGCET 2018 at Denmark..

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)