Emerging Security Protocols in Wireless Sensor Networks

Keshvi Khambhati, Dr.Kakelli Anil Kumar

Abstract: ***Wireless Sensor Networks (WSN) is falls under overwhelming and surging technology that shows extraordinary guarantee for different advanced potential applications like military, atomic power plant, human services and so forth, where security is a basic issue. These systems are generally utilized as a part of different conditions that likewise incorporates open condition, unattended nature, a few asset limitations, remote and shared correspondence, un-trusted and broadband transmissions between them, that have different imperatives like low calculation ability, restricted memory, decreased battery existence, absence of foundation that forces safety as an extra difficult undertaking. In this paper a point-by-point examination on the safety related problems in WSN are made. Likewise, a brief on different security systems with proficient power conservation procedures is shown in a table. Comparison of all the security protocols are based on the technique used to give security in wireless sensor networks, the framework used or model used, the key mechanism they are using to provide the best security they can give, which all performance parameters they are improving in terms of energy consumption or increasing network age or reducing some unwanted network performance affecting characteristics and also on what kind of security they are providing and up to which extend they are providing security while transmitting the packets from one end to other end.***

Index Terms: Security Protocol, Sensors, Wireless Sensor Networks

I. INTRODUCTION

Wireless sensor networks are having distributed connected sensor systems made up of geographically appropriated self-governing. The components of a sensor node are microcontroller, memory, control originator and antenna. WSN has preferably utilized for military, environmental, medical, agriculture and robotic applications. Safeguarding the correspondences in these use case scenarios is a critical problem in light for the fact that the vulnerabilities in WSN, for example, listening in, ridiculing, physical trade off, message Trustworthiness, geo area and forswearing of administration. Importance is to be given to from source to destination data security and furthermore the calculative constraint limits decision of the encrypting calculations as well as conventions. Moreover, the existence of batteries for sensor nodes utilizing cryptography decreases the lifetime of sensor node. There are a few important security management protocols in wireless sensor systems like SPIN [1] which comprises of two secure building squares: SNEP [2] and the other protocol named µTESLA [3]. Between both of the above, SNEP incorporates data security, di-party data approval, as well as confirmation of data integrity. µTESLA offers cryptography and medium access control (MAC) schemes where symmetric key is utilized and it considers freshness (CTR) amid transmission. TinySec [4] gives administrations like SNEP, including confirmation, respectability of messages, protection and replay shield. A noteworthy distinction amongst SNEP and TinySec is nonattendance of counters that were utilized as a part of TinySec. TinySec deals with encryption and utilizations MAC amid transmission in remote sensor systems and uses any kind of key. MiniSec [5] is a sheltered and sound system layer convention that requires bring down vitality. Utilization than TinySec while accomplishing security level which is comparable with Zigbee. MiniSec gives freshness (CTR), encryption and utilizations MAC and any key course of action component for transmission. MiniSec gives verification to anchor transmission in remote sensor systems. LEAP [6] is designed for WSNs to help anchor interchanges for sensor models; subsequently, it gives the essential insurance administrations like, protection and acceptance. Zigbee [7] coordinator carries on as trust manager, which enables different gadgets to connect the system and furthermore disperses the keys. It assumes the three parts as trust, network and configuration supervisor. Furthermore, gives encryption, CTR, utilizations MAC and trust focus as a key course of action instrument. There are likewise a few different schemes like Secure Hybrid DFCMT scheme [8], where the primary highlights incorporate effective key communicate without retransmission/ACK, validation of key revelation without acquiring additional cost, recognize the lost keys, key refreshment without disturbing continuous information encryption/unscrambling. Schemes like LEDS, LLSP [8],[9] are additionally utilized for giving security in the remote wireless sensor networks (WSN). The comparison of all these security protocols are given in table 1. These protocols have better adjust of vitality utilization with security than that of past protocols. Be that as it may, vitality protection is an essential issue for accomplishing WSN security. Numerous researchers have demonstrated that key administration devours more battery vitality. In spite of the fact that extensive research is completed here, a productive vitality safeguarding encryption strategy for overseeing keys is now left to take it to an advanced level. This paper gives an itemized examination on the security problems, solutions and limitations of WSN. Likewise, a correlation on different security structures considering effective vitality protection strategies is said.

Table 1: Comparison of security protocols

Revised Manuscript Received on July 05, 2019.

Keshvi Khambhati, MTECH-SCOPE,VIT,Vellore,India.
Dr. Kakelli Anil Kumar,SCOPE,VIT,Vellore,India.

	MAC Used	Encryption	Freshness(CTR)	Overhead(Bytes)	Key Agreement
SPINS	YES	YES	YES	8	SYMMETRIC DELAYED
MINISEC	YES	YES	YES	4+3	ANY
802.15.4	YES	YES	YES	4,8 OR 16	-
ZIGBEE	YES	YES	YES	4,8 OR 16	TRUST CENTER
TINYSEC	YES	YES	NO	4	ANY
LEAP	YES	YES	NO	VARIABLE	PRE-DEPLOYED

II. BACKGROUND STUDY

A. Constraints In WSN

The major constraints in WSN as compared to normal networks when transmission of data is concerned are as follows[10]-[12]:

- Asset requirements: Wireless Sensor hubs have restricted resources, also having less computational ability, small storage, less unconnected correspondence message transmission, and a restricted, more often than not no rechargeable battery.
- Little message measure: Messages sent/received in wireless sensor networks arranges as a standard rule and thus have a small size unconventional and the current structure where there is no scope for adding any security bites/bytes as well as any other extra information for synchronization or for other purposes as been added with the message in other non-wireless networks.
- Tending to Schemes: Due to generally vast number of sensor hubs, it isn't conceivable to produce overseas moving to plans for organization of an extensive count of sensor nodes as aloft of character support is high. As the energy is very low in these kinds of networks, the far transmission of messages is an issue.
- Sensor area and excess of information: Position familiarity with sensor organize is major since data assembling is regularly in eye of region. This constraint comes under design constraints, where the network topology, moving nodes localization if
- any needs to be taken care of , as positioning of cluster heads and other nodes and all are to be considered for transmission.

B. Threat Models Of WSN

According to Karlof et al. [13] , Threats in wireless sensor network are divided into the areas mentioned below[14]-[18]:

- Outsider versus insider attacks: The outsider attacks respect assaults from hubs which don't have a place with a WSN. A pariah aggressor has no entrance to most cryptographic materials in sensor arrange. The insider attacks happen when honest to goodness hubs of a WSN act in unintended or unapproved ways. Within aggressor may have incomplete key material and the trust of other sensor hubs. Inside attacks are substantially harder to distinguish.
- Passive versus active attacks: The attacks called passive attacks are in the idea of listening stealthily on, or checking of parcels traded inside a environment called WSN; The dynamic attacks include a few adjustments of the information burst or the production of a not true burst in a WSN.
- Mote-class versus laptop-class attacks: In the attacks called mote class, a foe attacks a WSN by using some of the nodes with almost equal tendencies as that of structure hubs. In PC attacks, a foe can use every more ground-breaking devices like PC, as well as so forth and also does considerably higher damage to a structure than a pernicious sensor node.

C. Security Requirements for WSN

According to Ritu Sharma et al. (2010) [19], The major cause of security services in WSN is safeguard data and properties from assaults and misbehavior. The requirements in WSN for security include:

- Data Availability: It guarantees that the administrations are constantly accessible under system even using the assault, for example, Denial of Service assault. Accessibility is of essential significance to keep up an operational system. Accessibility guarantees that a sensor hub remains constantly dynamic in the system to satisfy the usefulness of the system.
- Authorization: Ensures that exclusive authorized sensors can be associated with giving data to organize administrations.
- Data Authentication: It guarantees that the information got by collector has not been adjusted amid the transmission. It is made possible through coherence or asymmetric techniques in which sender and collector nodes share secret keys.
- Data Confidentiality: Confidentiality intends to secure information amid correspondence in a system to be comprehended other than expected beneficiary. Cryptography procedures are utilized to give privacy. It is the a standout amongst the most imperative issue in arrange security.
- Data Integrity: It is exceptionally pivotal in sensor system to guarantee the unwavering quality of the information. It guarantees that information parcels that are gotten by the goal are precisely the ones sent by the sender and any one can't adjust that bundle in the middle.
- Non-repudiation: Denotes that a hub can't deny communicating something specific it has already sent.
- Data Freshness: It guarantees that the information got by the recipient is latest and crisp information as well as none of the enemy can again play the previous information. It's accomplished utilizing systems like random number or adding time signature to every datum parcel.
- Robustness- When a few hubs are endangered the whole system ought not be imperiled.
- Self-organization-Nodes ought to be sufficiently adaptable to act naturally arranging (self-governing) and self-recuperating (disappointment tolerant).
- Time Synchronization- These mechanisms ought not

be controlled to create erroneous information.

D. Security Related Attacks For WSN

As WSN discovers an extensive variety utilizations particularly in the area of protection, army, atomic energy plant and so on safety assumes a crucial part. As the security saving strategies is getting advanced, the sorts of interruption and ridiculing components additionally are being expanded. Objective related to safety benefits in WSNs is giving insurance to the data notwithstanding when mediation of different aggressors being available, with little vitality utilization as well as upgraded arrange lifetime.

- Denial of Service (DoS) [20]: In this type of assault, the programmers' goal is to render target machines unavailable by authentic clients. There are two sorts of DoS assaults: Passive assault: Selfish hubs utilize the system yet don't collaborate, sparing battery life for their own interchanges, they don't mean to specifically harm different hubs. Dynamic assault: Malicious hubs harm different hubs by causing system blackout by apportioning while at the same time sparing battery life isn't a need. Dos assaults can occur in various WSN conventions layers. In physical layer, this attack behaves to be not erasing and hardening, at interface level, impact, exhaustion, injustice, at organize level, ignore and keenness, homing, dilemma, not bright gaps as well as in transport level, this assault is performed by pernicious bursting as well as desynchronization. The structures to forestall DoS assaults includes portion for assembling assets, solid confirmation and recognizable proof of activity and pushback.
- Assaults on Information in Transit (Eavesdropping assault) [21]: The most widely recognized assaults against WSNs are on data in travel between hubs. Data in travel is defenseless against listening in, change, infusion that can be anticipated utilizing settled secrecy, confirmation, respectability and replay insurance conventions. Movement investigation can possibly be a major issue in WSNs enabling an aggressor to delineate directing design of a system, empowering firmly focused on assaults to disturb picked segments of a system for most prominent impact.
- Node Replication Attack [21]: A hub replication assault includes an aggressor embedding's another hub into a system, which has been cloned from a current hub, such cloning being a moderately straightforward undertaking with current sensor hub equipment. The mentioned fresh hub can behave precisely similar to the previous hub else can have some additional conduct, for example, transmitting data of intrigue specifically to the assailant. A hub replication assault is not kidding when the base station is cloned. In any case, with respect to numerous organizations, the base station is both in a protected area and significantly greater than whatever remains of the sensor hubs, so cloning it is substantially more troublesome.
- Routing attack [22]: Likewise with all systems there are various assaults that objective the directing convention of WSNs, which are all essentially insider assaults. Some are as per the following:
  1. Selective forwarding : This is a way to influence the structure activity by relying that all taking an interest hubs in arrange are loyal to pass the data. Malignant or assaulting hubs can decline to course certain messages and drop them. On the off chance that they drop every one of the parcels through them, at that point it is known as a black hole assault. In any case, in the event that they specifically forward the parcels, at that point it is called particular sending. Viability of this assault depends on two elements. To begin with the region of the malignant hub, the less far it is to the source station the higher movement it will pull in. In the Second level , the data is dropped.
  2. Sinkhole attacks: In this type of assaults, foe takes near in the rush period gridlock to a compromised off hub. The very less complex way for making sinkhole is to keep a noxious hub where it can make a majority of the activity, perhaps not far to the base station or malevolent hub itself beguiling as a base station.
  3. Sybil attacks: In Sybil attack, a solitary hub introduces numerous personalities to every single other hub in the WSN. This may deceive different hubs, and subsequently courses accepted to be disjoint w.r.t hub can have a similar enemy hub. Sybil assaults are sometimes used against steering computations and topology upkeep; which decreases the chances of blame tolerant plans, like, conveyed capacity and disparity.
  4. Wormholes: In this type of attacks, an enemy placed close to the source station can fully trick the motion using messages over a less inertness interface. In this case an intruder persuades the hubs which seems to be multi bounce away that they are nearer to the base station.
  5. Flooding: At some point, pernicious hub can cause colossal activity of futile information on the system. This is called as flooding. Occasionally, malevolent hubs replay some genuine communicate messages, and subsequently producing futile activity on the system. This can cause blockage, and may in the long run prompt the fatigue of finish hubs. This is a type of Denial of Service assault.
  6. Jamming (Radio Interference) Attack: In the most straightforward type of sticking, the assailant undermines the transmitted messages by causing electromagnetic mediation in the system's operational frequencies, and in vicinity to the

focused on recipients. An aggressor can honorably remove the connection among hubs by conveying persistent radio flags so other approved clients are not permitted to get to a specific recurrence channel.

7. Identity related attacks: In general, these assaults collaborate with listening in assaults or other system sniffing programming to accomplish powerless MAC and system addresses. They focus on the confirmation element.
8. Impersonate attack: An assailant mimic another hub's character (either MAC or IP address) to set up an association with or dispatch different assaults on a sufferer; the aggressor may likewise utilize the casualty's personality to build up an association with different hubs or dispatch different assaults in the interest of the casualty.

9. Security in wireless sensor systems is a basic issue keeping in see restrictions and application areas of sensor systems. In sensor organizes there is have to keep up a fragile harmony amongst security and system activities. The strategies, for example, Link Layer encryption and validation, multipath steering, personality confirmation and verified communicate appear to be great answer for security in WSN. Anyway, assaults, for example, Sinkhole and Wormholes posture parcel of difficulties to anchor directing convention outline. Topographical Routing Protocols is one case of directing conventions, which can withstand the majority of the WSN steering based assaults, as the true blue hubs can assess the area of the foe hubs. Consequently, assaults, for example, Sybil are compelling. Compelling and Efficient countermeasures are yet missing against these assaults, which can be connected after the plan of these directing conventions has finished. So there exist a serious need to outline such steering conventions in which these assaults are insufficient.

III. EXISTING SECURITY SOLUTIONS IN WIRELESS SENSOR NETWORKS

Below are various security solutions are proposed which are used for serving the purpose of providing security solutions with energy efficiency for data transmission [30].

Sonia, Kusum Dalal., 2016 has proposed a various leveled protocol [31], which manages security heterogeneity, in light of LEACH. In the system, there are various sensor nodes (SNs) and a base station (BS). A Symmetric key cryptographic administration strategy had been used so as to upgrade the security of WSN organize. There is a couple shrewd key is doled out to every hub match called two-way keys. A partner will utilize the key regular with relating cluster head CH to speak with it. CH will utilize MC (manufacturing code) to speak with base station BS. Amid the setup stage some noxious hubs are recognized. Also, the right code, ID or key gets flowed to all the relating hubs. If a hub sends ready messages more than some edge esteem then BS asks a bundle from the alarming hubs and that hub which are cautioning them. In ask parcel, id, code, and hashed keys are required then BS thinks about these qualities as its own. On the off chance that there is any befuddle for a specific hub at that point boycott that node. The lifetime of hubs is likewise expanded utilizing the above method, as malevolent hubs are prohibited on introductory stage subsequently less power is devoured in arrange. In this way the system works in a more vitality productive way.

Huang Lu et al., suggested two Secured and Efficient information Transmission (SET) conventions [32] called SET-IBS and SETIBOOS in 2014 to decrease the calculation and capacity expenses of mark preparing. SET-IBS (Identity Based advanced Signature) and SET-IBOOS (Identity Based /Offline Signature) are for the most part used to confirm the scrambled detected information by computerized marks. These two protocols proposed above can rely upon the Identity root cryptography and client open keys are their Identification data. Consequently, clients get the relating private clue with no information conveyance, which is productive in vitality sparing. These two protocols proposed above have a naming instatement preceding structure arrangement and functions in turns which comprises, set up stage for framing groups from Cluster heads and a consistent being stage for conveying information from Source Nodes to the Base Station in each round. It demonstrated better execution as far as security overhead and vitality utilization when contrasted and other existing security conventions.

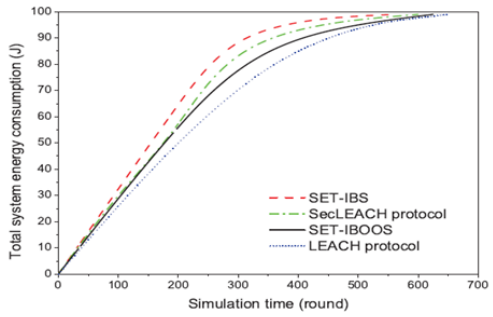

Fig 1. Energy Consumption of SET-IBS and SET-IBOOS protocol

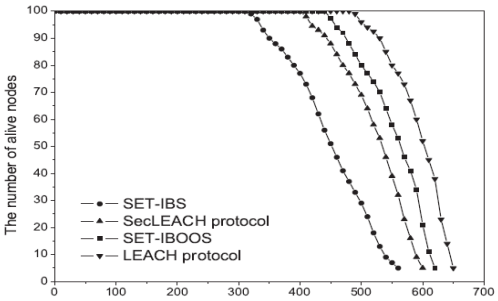

Fig 2. Number of alive nodes of SET-IBS and SET-IBOOS protocol

Di Wu, Gang Hu , Gang Ni., 2008 have proposed a routing convention which improves the security amid transmission of data. The SS-LEACH [33] calculation is a three-stage convention which makes utilization of hubs self-limitation innovation and keys pre-conveyance procedure. This Protocol calculation, that is implemented using this paper, additionally separates the whole system into groups. Be that as it may, the race of group heads bases on the rest of the vitality and the separation between hubs. Furthermore, the separation can be figured independent from anyone else restriction innovation, yet not "hops". So, it can stay away from separate mistake. It boosts the method of picking some heads for a group of nodes and structures non-static stochastic multi-ways group heads chains. The SS-LEACH convention can oppose the particular sending attacks, Sybil attacks and HELLO surge attacks adequately. The reproduction result demonstrates that the hubs passed on afterwards in proposed protocol than in LEACH consequently shows that the proposed protocol calculation not just delays the age of remote sensor arranges successfully, yet additionally improves steering security emphatically.

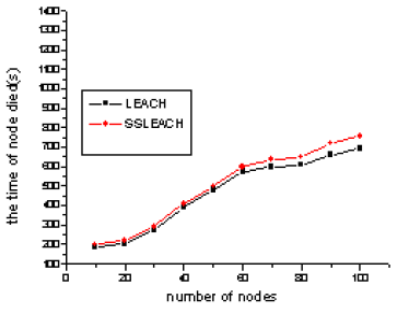

Fig 3. Time of nodes Died of SS-LEACH as compared to LEACH Protocol.

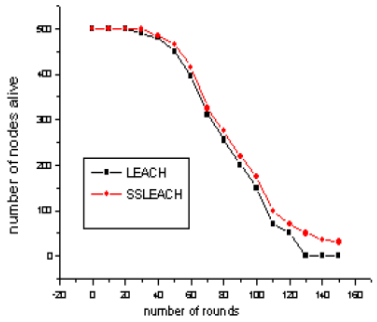

Fig 4. Comparison of Network Lifetime of SS-LEACH vs LEACH protocol.

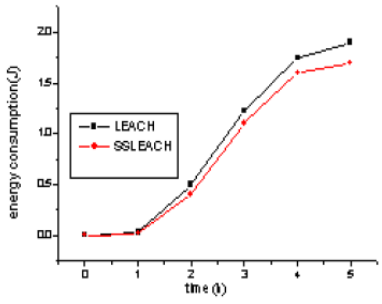

Fig 5. Energy consumption of Cluster Head of SS-LEACH vs LEACH protocol.

Gopi saminathan et al., 2013, proposed a convention upgraded DAO LEACH [34], which guarantees privacy of totaled information. GDDA plot depends based considering Locality Sensitive Hashing (LSH) method for building the information total exactness and the codes are produced by the Source Nodes to diminish the quantity of bits to be conveyed. HLUA conspire comprises of a mix of MAC calculation and ECC calculation. Macintosh calculation is utilized to satisfy bring down energy request in middle of the Cluster Heads and Source Nodes. ECC calculation are connected amongst Cluster Heads and utilizers for User validation. Upgraded DAO-LEACH convention stays away from replay attacks, hub trading off attacks and pantomime attacks. It demonstrated better execution as far as Aggregation exactness, Count of hubs not dead, Total Delay, False information discovery and Power utilization.

N.S. Fayed., E.M. Daydamoni, A. Atwan., 2012 presented a joined safety framework to aid WSN which upgrade the fastness of the system and it's vitality utilization. This framework consolidates two in number conventions [35], Less weighted Kerberos and Elliptic Curve Menezes– Qu–Vanstone (ECMQV). The entire system is isolated into progressive structure and from base station to layer 2 (sensor nodes) the lightweight Kerberos is utilized and from layer 2 (sensor hubs can impart utilizing 2 hops) to layer 3 (sensor nodes can convey utilizing 3 hops) Authenticated Diffie Hellman is utilized. Less weighted Kerberos convention with small messages is connected with little system and ECMQV convention on the extensive one. But the greater part of conventions utilizes third equality, as Kerberos is a protocol which has a three-route correspondence since 2 substances hoping to set up mystery clue don't just send/receive information to each other yet additionally to the confided in specialist. Hence, the correspondence vitality value for Kerberos conventions is considerably more than the vitality required for figuring encrypted natives. The consolidating framework takes the advantages of the two conventions. One of framework benefits is upgrading the vitality utilization. Sparing vitality implies diminishing count of correspondences and calculations, as well as this enhance the fastness of the system. Another advantage is, utilizing two in number conventions as Less weighted Kerberos and ECMQV enhances system safety. The exploratory consequences of the framework contrasted and vitality cost of Lightweight Kerberos and ECMQV Protocols demonstrated that, the general vitality cost of utilizing the joined framework is little that utilizing of Less weighted Kerberos or ECMQV considering them alone. The reproduction comes about exhibit that the consolidated framework can augment the existence time for remote sensor systems, improve its security, and increment its speed.

In 2009, Shih-I Huang et al., invented Safe encrypted information gathering technique [36] to take out excess sensor information without using cryptography, keeps up protection as well as mystery for information with diminished correspondence overhead. The above plan comprises of 2 stages: information cryptography and information

accumulation. The information crypto graphical stage utilizes a lightweight encryption calculation to give security and mystery to data send/receive. Crypto graphical calculation utilizes x-or and hashing work. Information conglomeration stage utilizes a technique to take out excess information from sensor hubs without keys are utilized as a part of this plan for encryption so known plaintext attacks, picked plaintext attacks, figure content just attacks and man-in-the-center attacks were maintained a strategic distance from.

TaoYang, XuXiangyang, LiPeng, LiTonghui, PanLeina., 2018 proposes an Energy with a specific end goal to contradict pernicious attacks from interior hubs in WirelessSN, the paper mentioned above invents an Energy-optimized-Secure-Routing (EOSR) [37] in light of conveyed trust assessment structure to recognize as well as confine Harmful hub. EOSR directing convention composed a many-factor routing system, considering the node's trust level, the rest of the vitality and way length. EOSR conventions incorporate trust assessment, route development and route upkeep. The trust assessment is in charge of figuring the trust estimation of the node in view of the hub's correspondence conduct. The course development thoroughly considers the trust estimation of the hub, the rest of the vitality as well as the hop numbers tally of way to locate a dependable with vitality adjusted route. At the point where a pernicious node is there or an inadequate vitality hub in the route, route support will tell the source-node to build up another sending path. This procedure not just guarantees that information is transmitted through the confided in node, yet additionally balances vitality utilization among the confided in nodes. By assessing the execution of EOSR and contrasting EOSR and EN-AODV10 and TARF11 comes about demonstrates that there is a superior execution of the EOSR directing convention from three viewpoints with deference from bundle conveyance rate, organize throughput and node normal vitality utilization.

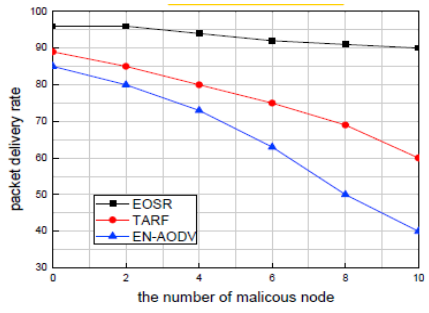

Fig 6. Packet Delivery Rate of EOSR vs TARF, EN-AODV

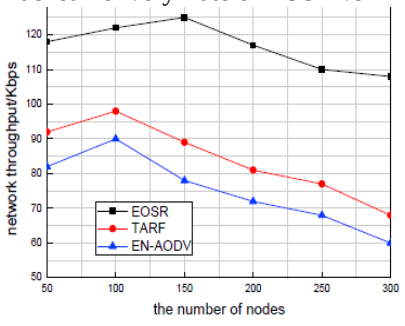

Fig 7. Network Throughput of EOSR vs TARF, EN-AODV

In 2013, Joyce Jose et aI, invented EPSDA [38] calculation for Wireless SN. EPSDA, which is called as Energy Efficient Privacy preserving Secure Data Aggregation keeps running on Network Simulator 2 for testing system. In which, information collection method joins information using various sensor hubs in view of total capacities by evading repetitive information. EPSDA accomplishes high data transmission and vitality effectiveness and subsequently, it expands the system lifetime. EPSDA produces another cryptographic key for each fresh session and it keeps again playing attack by accomplishing information newness amid collection. The conglomeration hierarchy was built utilizing the Tiny Aggregation (TAG) convention. Every leaf hub cuts the information divided in m no. of pieces and scrambles all cuts utilizing the cryptography key of the hub. At that point each leaf hub aggregates up the scrambled cuts got from surrounding hubs. MAC was created amid the procedure of information accumulation. Scrambled information with MAC is being sent to the BS. At that point, BS checks the amassed MAC got using the structure using the MAC produced from the unscrambled accumulated outcome. In the event that real contrast was discovered, at that point the sink presumed that the alteration was happened amid conglomeration and rejects the total outcome. EPSDA permits just a single unscrambling task on sink hub and ensures all the safety necessities with negligible correspondence and calculative overhead.

Priyanka Ahlawat, Mayank Dave., 2017 presents an exceedingly secure key administration scheme [39] in light of an effective attack display for cell model of systems. The attack display is composed in view of the situation of the sink in cell and neighbor impact factor. Thus, this creates it productive to keenly manage hub catch attacks in such systems. In this Scheme, the hash chain key pre-conveyance period of the proposed plot is processed utilizing the assessed trade off likelihood of every cell ahead pre-disseminating the available keys in hubs, a grid-rooted attack display is developed and bargain likelihood of every cell is afterwards registered. The entire bunch of keys being separated in to m sub-key bunches where m is the aggregate count of cells. A 2-Dimension hashed chain is then made in view of the tradeoff likelihood of every cell. Every hub of similar cell is accepted to have similar trade off likelihood. In a key which is shared revelation, the hubs communicate their key ids alongside the estimation of hashed work. Along these lines, the keyed bunch of cells that are higher inclined to attacks being set toward the finish of hashed chain. This outcome for minimum estimation of likelihood of key trade off. Further, the re-keying overhead is additionally lessened in proposed conspire as number of affected hubs is slightest. It at last prompts minimum number of connections rekeyed. In proposed plot, center is around two issues that how we can build the opposition of the framework without diminishing the hub network. The outcomes demonstrate that the proposed plot is profoundly secure to hub catch attacks.

In 2014, Madhumita Panda invented two open key rooted calculations [40], RSA as well as ECC to recognize a

reasonable encryption method to be used in WSN. The disadvantage of Symmetric key encryption is that it doesn't increase or decrease in number well if the quantity of hubs develops. Hilter kilter cryptography additionally called as Public-key Encryption utilizes these two, open and private key for information encryption as well as decoding, also it goes out on a limb of the key-sharing and here is the private-key is never uncovered. ECC calculation principally relies upon the arithmetical model of elliptical bends as well as the advantage of the above calculation is the littler key length and decreased stockpiling prerequisites. Subsequently contrasted and RSA, it has more noteworthy consideration as a security answer for WSN. Detailed comparison about all the above mentioned security protocols are mentioned in above Table 2.

Table 2: Detailed Information About Available Security Frameworks For WSN

Author/Year	Techniques Used	Framework	Keys mechanism	Performance Matrices	Security Provided
Tao Yang, Xu Xiangyang一, Li Peng, Li Tonghui, Pan Leina., 2018	Beta distribution, routing request frame (RREQ) and routing reply frame (RREP) of the AODV protocol	Energy optimized Secure Routing (EOSR).	Beta based Trust Evaluation key	Network Throughput, Packet delivery rate, Node average energy consumption	Only allows transmission through Trusted node.
Priyanka Ahlawat*,Mayank Dave., 2017	Hash chaining Function, compromised probability of nodes, Rekeying	Highly secure key management model	Hash chain of keys	Key compromise, rekeying overhead of links	Resistant to Node capture attacks
Sonia, Kusum Dalal., 2016	Symmetric key cryptography	Hierarchical protocol based on LEACH	Hash based symmetric key	Network lifetime, Energy efficient, reduced network disruption	Malicious nodes are detected in advance thereby reducing the risk of network disruption
Huang Lu et al.,2014	IBS and IBOOS scheme	SET-IBS and SET-IBOOS	ID based key	Network lifetime, The number of alive nodes, Overall system energy problem.	It lessens HELLO flood, It settles Orphan node problem
Madhumita Panda., 2014	RSA and ECC	Public key-based algorithms	Private and Public key	Communication overhead, Energy Consumption	It offers good trade-off between security and size of the key used.
Gopi saminathan et al., 2013	ECC and MAC	Enhanced DAO LEACH	Public and Secret key	False data detection, Energy Consumption, End to End Delay, Number of nodes alive, and aggregation accuracy	It is impervious to replay attacks, impersonation attacks and node compromising attacks
Joyce Jose et al., 2013	MAC	EPSDA (Energy Efficient Privacy preserving Secure Data Aggregation)	Changing Encryption key for every session	Communication overhead, Accuracy, Computational overhead, Energy Consumption	It lessens the replay attacks and the prevalence of the node compromising attack.
N.S. Fayed , E.M. Daydamoni, A. Atwan., 2012	Lightweight Kerberos and Elliptic Curve	Efficient combined security system	Elliptic curve-based key Exchange and	Energy efficient, Low computation, Low network	Provides energy efficient Authentication

	Menezes–Qu–Vanstone (ECMQV)		Kerberos key distributio	overhead, Low Power consumption	mechanism
Shih-I Huang et al., 2009	Irreversible Hash Function	Secure encrypted-data aggregation technique	Random keys	Efficiency, Communication overhead	It is strong to Known-plaintext attacks, chosen-plaintext attacks, cipher, text-only attacks and man-in-the-middle attacks
Di Wu, Gang Hu , Gang Ni., 2008	Node self-localization technology and Key pre-distribution strategy	SS-LEACH	Shared Random keys	Network Lifetime, Energy Consumption of cluster head, Node Lifetime, Two imperative goals	It resists selective forwarding attacks, Sybil attacks and HELLO flood attacks effectively.

IV. CONCLUSION AND FUTURE WORK

Security protocols have Crucial importance for all WSN applications. We have investigated and presented the strengths and weakness of various security protocols of WSN. These security conventions can work productively to give security to WSN. Security problems arise continually in WSN that should be broke down in deep to configuration appropriate security solutions and prevent the security problems. What's more, this exploration paper gives an outline of safety related problems and difficulties inside WSN as well as the current structures. While executing security methods by considering the confinements that influence the productive task of WSN more difficulties that should be thought about to assemble proficient WSN.

As there are a lot of already available security protocols which are serving the purpose of secure transmission of messages sent across the wireless sensor networks, a new protocol which can serve the purpose of providing energy efficiency as well as high security to WSN is to be looked upon. By implementing the concept of secondary cluster head logic along with trust factor for transmission makes the protocol strong for wireless sensor networks with respect to security as well as energy efficiency. Secure multipath communication is another strategy to achieve energy efficient secure communication.

REFERENCES

1. S. Juneja, "Performance Analysis of SPIN and LEACH Routing Protocol in WSN," International Journal of Computational Engineering Research (ijceronline.com), 2012.
2. S. Islam, "Security Property Validation of the Sensor Network Encryption Protocol (SNEP)," Computers, 2015.
3. N. Ruan and Y. Hori, "DoS attack-tolerant TESLA-based broadcast authentication protocol in internet of things," in 2012 International Conference on Selected Topics in Mobile and Wireless Networking, ICOST 2012, 2012.
4. U. Iqbal and S. Intikhab, "Re-keying mechanism for TinySec using ECC and Hash chains," in 2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017, 2017.
5. J. Panghal and N. Verma, "A Review on Security Analysis in WSN," International Journal of Recent Research Aspects, 2016.
6. M. Yassine and A. Ezzati, "LEAP enhanced: A lightweight symmetric cryptography scheme for identifying compromised node in WSN," International Journal of Mobile Computing and Multimedia Communications, 2016.
7. S. Md Zin, N. Badrul Anuar, M. Laiha Mat Kiah, and A. S. Khan Pathan, "Routing protocol design for secure WSN: Review and open research issues," Journal of Network and Computer Applications. 2014.
8. R. P. Manohar and E. Baburaj, "Secure Hybrid DFCMT scheme for Dynamic Routing in Wireless Sensor Networks," International Journal of Computer Science and Network Security, 2016.
9. K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks," IEEE Transactions on Mobile Computing, 2008.
10. N. Gupta, N. Kumar, and S. Jain, "Coverage problem in wireless sensor networks: A survey," in International Conference on Signal Processing, Communication, Power and Embedded System, SCOPES 2016 - Proceedings, 2017.
11. S. M. Mohamed, H. S. Hamza, and I. A. Saroit, "Coverage in mobile wireless sensor networks (M-WSN): A survey," Computer Communications. 2017.
12. D. V. Queiroz, M. S. Alencar, R. D. Gomes, I. E. Fonseca, and C. Benavente-Peces, "Survey and systematic mapping of industrial Wireless Sensor Networks," Journal of Network and Computer Applications. 2017.
13. Chris Karlof and David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures",Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 2003.
14. J. Granjal, E. Monteiro, and J. S. Silva, "Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey," Ad Hoc Networks. 2015.
15. A. Di Mauro, D. Papini, R. Vigo, and N. Dragoni, "Toward a Threat Model for Energy-Harvesting Wireless Sensor Networks," in Communications in Computer and Information Science, 2012.
16. G. Wu, X. Chen, L. Yao, Y. Lee, and K. Yim, "An efficient wormhole attack detection method in wireless sensor networks," Computer Science and Information Systems, 2014.
17. L. Chhaya, P. Sharma, G. Bhagwatikar, and A. Kumar,

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

"Wireless Sensor Network Based Smart Grid Communications: Cyber Attacks, Intrusion Detection System and Topology Control," Electronics, 2017.

18. S. Ben Othman, A. A. Bahattab, A. Trad, and H. Youssef, "Confidentiality and Integrity for Data Aggregation in WSN Using Homomorphic Encryption," Wireless Personal Communications, 2014.
19. Ritu Sharma, Yogesh Chaba and Yudhvir Singh,"Analysis of Security Protocols in Wireless Sensor Network",Int. J. Advanced Networking and Applications 2010.
20. P. Gope, J. Lee, and T. Q. S. Quek, "Resilience of DoS Attacks in Designing Anonymous User Authentication Protocol for Wireless Sensor Networks," IEEE Sensors Journal, 2017.
21. H. N. Dai, Q. Wang, D. Li, and R. C. W. Wong, "On eavesdropping attacks in wireless sensor networks with directional antennas," International Journal of Distributed Sensor Networks, 2013.
22. M. Tripathi, M. S. Gaur, and V. Laxmi, "Comparing the impact of black hole and gray hole attack on LEACH in WSN," in Procedia Computer Science, 2013.
23. S. M. Sajjad, S. H. Bouk, and M. Yousaf, "Neighbor node trust based intrusion detection system for WSN," in Procedia Computer Science, 2015.
24. P. Dewal, G. S. Narula, V. Jain, and A. Baliyan, "Security attacks in wireless sensor networks: A survey," in Advances in Intelligent Systems and Computing, 2018.
25. J. Wu, K. Ota, M. Dong, and C. Li, "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities," IEEE Access, 2016.
26. M. Bendjima and M. Feham, "Wormhole attack detection in wireless sensor networks," in Proceedings of SAI Computing Conference, SAI, 2016.
27. Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," IEEE Transactions on Mobile Computing, 2014.
28. J. Srinivas, S. Mukhopadhyay, and D. Mishra, "Secure and efficient user authentication scheme for multi-gateway wireless sensor networks," Ad Hoc Networks, 2017.
29. A. Diaz and P. Sanchez, "Simulation of attacks for security in wireless sensor network," Sensors (Switzerland), 2016.
30. Anita-Daniel.D, Emalda-Roslin.S ,"A Review on Existing Security Frameworks with Efficient Energy
Preservation Techniques in Wireless Sensor Networks", IEEE ICCSP 2015 conference
31. Sonia and Kusum Dalal,"Security Enhancement in
WSN Networks used Cryptography Techniques", IJRTER june-2016 Vol 02, Issue 06
32. Huang-Lu, Jie-Li,Mohsen-Guizani, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks", IEEE, march 2014.
33. Di-Wu,Gang, Hu,Gang-Ni,"Research and Improved on Secure Routing Protocols in Wireless Sensor Networks",IEEE 2008.
34. Gopi Saminathan and S-Karthik, "Development of an energy efficient, secure and reliable Wireless Sensor Networks Routing Protocol based on Data Aggregation and user Authentication" , American Journal of Applied Sciences 10 (8).
35. N.S.-Fayed, E.M.-Daydamoni and A. Atwan,"Efficient combined security systems for wireless sensors network",Egyptian Informatics Journal (2012)
36. Shih-I.Huang, Shiuhpyng-Shieh and J.D.Tygar, "Secure encrypted-data aggregation for Wireless Sensor Networks", Springer May-2009.
37. Tao Yang, Xu Xiangyang ─, Li-Peng, Li-Tonghui and Pan-Leina,"A Secure routing of wireless sensors protocol based on trust evaluation model",8th ICICT-2018.
38. Joyce-Jose, M-Princy,Josna-Jose, "EPSDA: Energy Efficient Privacy preserving Secure Data Aggregation for Wireless Sensor Networks", IJSA Vol. 7, No. 4, July, 2013.
39. Priyanka-Ahlawat and Mayank-Dave,"An Attack models based on Highly secure key management scheme for wireless sensor networks",6th ICSCC-2017.
40. Madhumita-Panda, "Security in Wireless Sensor Networks using Cryptographic Techniques", AJER 2014.