ISSN No. 0976-5697

Volume 4, No. 11, Nov-Dec 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Secure Aggregation in Wireless Sensor Networks: A Review

Rakesh Sharma
Department of Computer science & Engineering, HCTM
Technical Campus Kaithal, Haryana, India
rakeshsharma3112@gmail.com

Matish Garg
Department of Computer science & Engineering, SBIET
Pundri, Haryana, India Kaithal, Haryana, India
matish26sep@rediffmail.com

Pinki Sharma
Department of Computer science & Engineering, HCTM
Technical Campus Kaithal, Haryana, India
pinkisharma@gmail.com

***Abstract*:** A wireless sensor network generally consists of huge range of inexpensive densely deployed detector nodes that have strictly forced sensing, computation, and communication capabilities. Due to resource restricted detector nodes, it is necessary to scale back the number of data transmission in order that average time period of detector and so the information measure consumption square measure improved. Knowledge aggregation is that the strategy of summarizing and mixing detector knowledge thus on minimizes the number of data transmission within the network. Wireless sensor networks square measure generally deployed in remote and hostile environments to transmit sensitive knowledge, detector nodes square measure in peril of node compromise attacks and security problems like knowledge confidentiality and integrity square measure very necessary. Therefore, wireless sensor network protocols, e.g., knowledge aggregation protocol, need to be designed with security. During this paper we have a tendency to investigate the link between security and knowledge aggregation methodology in wireless detector networks.

Keywords: knowledge aggregation, WSN, Security, DOS, Extended Kalman Filter.

I. INTRODUCTION

Wireless sensor networks square measure generally composed of immeasurable low value, weak sensing sensors with restricted storage, process and communication resources [1], [2], and [21]. These networks provide most likely low cost solutions to associate issues in each military and civilian application, what is more as field of battle work, target trailing, environmental and health care trying, inferno detection, and traffic regulation. Due to the low implementation expenditure wants of wireless detector networks, detector nodes have simple hardware and severe resource constraints [24]. Hence, it's a troublesome task to produce economical solutions to knowledge gathering issues. Among these constraints, ‘‘battery power” is that the foremost limiting issue that takes into consideration within the formation of wireless detector network protocols.

Consequently, to reduce the facility consumption of wireless detector networks, many mechanisms square measure planned like radio programming, management packet elimination, topology management, and most significantly knowledge aggregation [2],[3]. Knowledge aggregation protocols aim to mix and summarize knowledge packets of the various detector nodes thus as that quantity of data transmission is reduced. Once the bottom station queries the network, rather than transfer every detector node’s knowledge to base station, one in all the detector nodes, referred to as knowledge soul, collects the data from its near nodes, aggregates them, and sends the mass knowledge to base station over a multi hop path. As illustrated by the instance, data aggregation reduces the number of data transmissions by this implies improve information measure and energy utilization among the network.

In wireless sensor networks, the advantage of knowledge aggregation can increase if the intermediate detector nodes perform data aggregation incrementally once the data is being forwarded to base station. Although this continuous data aggregation operation improves the info information measure and energy consumption, it needs to negatively have a sway on different performance metrics like delay, accuracy, fault-tolerance, and security [3]. As a result of the majority of wireless detector network applications need a precise level of security, it's impossible to sacrifice security for knowledge aggregation. In addition, there's a strong conflict between security and data aggregation protocols. Security protocols need detector nodes to ciphers and certify any perceived knowledge before its transmission and like knowledge to be decrypted by base station [12], [20]. On the choice hand, knowledge aggregation protocols like plain knowledge to implement knowledge aggregation at each intermediate node so energy potency is maximized. Besides, knowledge aggregation leads to alterations in detector knowledge thus it's a troublesome task to produce data authentication in conjunction with knowledge aggregation. Due to these contradictory goals, data aggregation and security protocols need to be designed on so as that knowledge aggregations square measure performed whereas not sacrificing security.

The need of implementing knowledge aggregation and security along attracts several researchers to figure on secure data aggregation drawback. Throughout this paper, we offer a radical review of secure knowledge aggregation thought in wireless detector networks by technique the foremost issues

and covering the foremost necessary add the world. Compared to general knowledge aggregation drawback that's a well researched topic in wireless detector networks, secure data aggregation drawback still has the potential to produce several fascinating analysis opportunities.

II. SECURITY REQURIMENT OF WIRELESS SENSOR NETWORKS

By reason of hostile environments and distinctive properties of wireless sensor networks, it is a tough task to protect sensitive knowledge transmitted by wireless sensor networks [21]. In addition, wireless detector networks have security issues that usual networks do not face. Hence, security could be an important issue for wireless sensor networks and there square measure many security considerations that ought to be investigated. Throughout this section, we have a tendency to tend to convey the essential security requirements that square measure raised in Associate in nursing extremely wireless sensor network setting and justify but these needs relate with data aggregation technique.

A. Data Confidentiality:

In wireless sensor networks, data confidentiality assure that secrecy of detected data isn't disclosed to unauthorized parties and it is the foremost important issue in mission essential applications. Authors of [17] state that a detector node mustn't disclose its readings to near nodes. Moreover, in many applications, detector nodes transmit sensitive data, e.g., secret keys; and so it's terribly important to form secure channels among detector nodes. Public detector data, like detector identities and public keys, need to even be encrypted to some extent to protect against traffic analysis attacks. Besides, routing data ought to put together keep confidential in certain cases as malicious nodes can use this data to degrade the network's performance. The quality approach for keeping sensitive data secret is to encode the information with a secret key that entirely supposed receivers possess, so achieving confidentiality. However, knowledge aggregation protocols generally cannot combination encrypted data. Therefore, such data aggregation protocols should decipher the detector data to perform data aggregation and write in code the combination data before causation it. This decryption/encryption of detector data at data aggregators not entirely results in delay and energy consumption but conjointly prevents end-to-end data confidentiality

B. Data integrity and freshness:

Although data confidentiality guarantees that entirely meant parties get the un-encrypted plain data, it doesn't defend data from being altered. Data integrity guarantees that a message being transferred isn't usually corrupted. A malicious node could corrupt messages to forestall network from functioning properly. In fact, as a results of untrustworthy communication channels, data might even be altered whereas not the presence of unwelcome person. Thus, message authentication codes or cyclic codes square measures custom-made forestall data integrity. Knowledge aggregation winds up in alterations of data; so, it's impractical to have end-to-end integrity check once knowledge aggregation is employed. Moreover, if Associate in nursing data collector is compromised, then it's attending to corrupt detector data throughout knowledge aggregation and conjointly the bottom station has no technique of checking the integrity of this mass detector data. Providing knowledge integrity is not enough for wireless communication as a result of compromised detector nodes square measure able to hear transmitted messages and replay them shortly to disrupt the info aggregation results. Data freshness protects data aggregation schemes against replay attacks by guaranteeing that the transmitted data is recent.

C. Authentication:

Since wireless sensor networks use a shared wireless medium, detector nodes need authentication mechanisms to find maliciously injected or spoofed packets. Supply authentication permits a detector node to substantiate the identity of the peer node it's communication with. Whereas not supply authentication, Associate in Nursing opposed would possibly masquerade a node, so gaining unauthorized access to resource and sensitive data and busy with the operation of various nodes. Moreover, a compromised node would possibly send data to its knowledge soul to several pretend identities so as that the integrity of the mass data is corrupted. Faking multiple detector node identities is known as Sybil attack and it poses important threat to data aggregation protocols [22]. If entirely two nodes square measure in communication, authentication may be provided by even key cryptography. The sender and therefore the receiver share a secret key to calculate the message authentication code (MAC) for all transmitted knowledge. However, data aggregators needs broadcast authentication that wants plenty of advanced techniques, like µTESLA [22].

D. Availability:

Availability guarantees the survivability of network services against Denial-of-Service (DoS) attacks. A DoS attack may be launched at any layer of a wireless senor network and should disable the victim node(s) for good. In addition to DoS attacks, excessive communication or computation could exhaust battery charge of a detector node. Consequences of accessibility loss might even be ruinous. As an example, throughout a field investigating application, if the supply of some detector nodes cannot be provided, this could cause Associate in nursing enemy attack. Wireless detector networks square measure deployed with high node redundancy to tolerate such handiness losses. Since data aggregators collect the info of form of detector nodes and sends the collective information to the bottom station, handiness of data aggregators is extra vital than regular detector nodes. Thus, in wireless detector networks, intruders launch DoS attacks with the aim of preventing data aggregators from acting their task thus that some a section of the network losses its accessibility.

III. KNOWLEDGEAGGREGATION

In a typical wireless sensor network, Associate in Nursing large vary of detector nodes collect application specific knowledge from the environment and this knowledge is transferred to a central base station where it's processed, analyzed, and employed by the applying. In these resource forced networks, the final approach is to put together technique the information generated by all completely different detector nodes whereas being

forwarded toward the bottom station [10]. Such distributed in-network process of knowledge is usually referred as data aggregation and involves combining the information that belong identical development. the most objective of data aggregation is to increase the network life by reducing the resource consumption of detector nodes (such as battery energy and bandwidth). Whereas increasing network life, knowledge aggregation protocols might degrade necessary quality of service metrics in wireless detector networks, like data accuracy, latency, fault-tolerance, and security.

Therefore, the planning of a cheap data aggregation protocol is Associate in nursing inherently tough task as a result of the protocol designer should trade off between energy efficiency, data accuracy, latency, fault-tolerance, and security. Thus on attain this trade off, data aggregation techniques square measure tightly as well as but packets square measure routed through the network. Hence, the planning of the detector network plays a major role among the performance of assorted data aggregation protocols. There square measure several protocols that change routing and aggregation of data packets at an equivalent time. These protocols may be categorized into two parts: tree-based knowledge aggregation protocols and cluster-based data aggregation protocols. Earlier work on data aggregation centered on up the prevailing routing algorithms thus on build knowledge aggregation getable. As a result, many data aggregation protocols supported shortest path tree structure has been planned to cut back the latency credit to tree-based data aggregation, recent work on data aggregation tends to cluster detector nodes into clusters so as that data square measure collective in each cluster for improved efficiency.

IV. SECURE DATA AGGREGATION

Like all different wireless detector network protocol, knowledge aggregation protocols ought to satisfy the security wants explained in Section 2. However, the resource affected detector nodes and necessity of plain data for aggregation technique cause challenges once implementing security and data aggregation on. A security demand of wireless detector networks is happy victimization either even key or uneven key cryptography. Owing to resource constraints of detector nodes, even key cryptography is most well-liked over uneven key cryptography. Hence, the need of implementing data aggregation and security victimization even key cryptography algorithms have light-emitting diode many researchers to work on secure knowledge aggregation drawback [1],[4],[9],[11],[14],[15],[17]-[20]. In these protocols, security and data aggregation square measure achieved on throughout a hop-by-hop fashion. That is, data aggregators ought to decipher each message they receive, combination the messages consistent with the corresponding aggregation perform, and encode the aggregation result before forwarding it. Additionally, these schemes would like data aggregators to establish secret keys with their near nodes. Therefore, hop-by-hop secure data aggregation protocols cannot provide knowledge confidentiality at data aggregators and finish in latency owing to the decryption/encryption technique. So as to mitigate the drawbacks of hop-by-hop secure data aggregation protocols, a gaggle of data aggregation protocols is planned [1].

The planned protocols perform data aggregation whereas not requiring the decoding of the detector knowledge at data aggregators. Whereas variety of those protocols use even cryptography, others use uneven key cryptography functions that square measure acceptable for resource affected detector nodes. As data aggregators don't need to be compelled to decipher detector data to perform aggregation, the protocols planned in [1] provide finish-to-end data confidentiality and end in less latency compared to hop by-hop secure data aggregation protocols. On the other hand, the cringe of the data aggregation protocols that don't would like the cryptography of detector information is that they are applicable to entirely a gaggle of aggregation functions, like add and average. Within the follows, we have a tendency to tend to c justify the secure data aggregation protocols supported the need of decrypting detector data at data aggregators.

A. Secure data aggregation victimization plain detector data:

Earlier work on secure data aggregation is targeted on even key cryptography and aggregation of plain data. In [20], the authors propose security mechanisms to find node misbehavior (dropping, modifying or formation messages, transmittal false combination value). The key arrange of this work is delayed aggregation. Instead of aggregating messages at the immediate next hop, messages square measure forwarded unchanged over the first hop thus mass at the second hop. This is often achieved using a key chain; the bottom station periodically broadcast authentication keys. Hence, detector nodes have to be compelled to buffer the data to manifest it once the authentication key broadcasted by the bottom station. The planned protocol ensures data integrity, and however it does not provide data confidentiality. Additionally, if a parent node and its child square measure compromised nodes, then data integrity is not secured either. A witness based data aggregation theme for wireless detector networks is projected in [19]. The witness nodes of every data soul in addition perform data aggregation and computes MACs of the combination data.

Witness nodes don't send their combination data to the bottom station. Instead, every witness node sends its MACs of the combination knowledge to the info soul. The info soul collects and forwards the MACs to the bottom station. Those MACs that square measure computed by the witness nodes square measure used at the bottom station for validate the correctness of the info combination by information aggregators. This enhances the support of information aggregation. Thus on prove the validity of the mass data, each data collector must provide proofs from several witnesses. As a result of the information validation is performed at the bottom station, the transmission of false knowledge and MACs up to base station affects adversely the employment of detector network resources. The projected protocol offers entirely integrity property to the information aggregation security. In [18], sampling mechanisms and interactive proofs square measure accustomed check the correctness of the mass knowledge at the bottom station. The projected protocol is termed SIA.

The authors claim that, by constructing economical sampling mechanisms and interactive proofs, it's attainable for the user to verify that the combination data provided by the collector could also be a sensible approximation of verity price even once the collector and a fraction of the detector nodes square measure compromised. specifically, the authors presents economical protocols for firmly

computing the median and therefore the average of the measurements, estimating of the network size, and finding the minimum and most detector reading. Among the paper, the correctness of data is checked by constructing a Merkle hash tree. Throughout this construction, all the collected data is placed at the leaves of the tree, and thus the collector computes a binary hash tree ranging from the leaf nodes: each internal node among the hash tree is computed as a result of the hash price of the concatenation of the 2 kid nodes. The foundation of the tree is termed the commitment of the collected data. The hash operate in use has got to be collision resistant. Once the collector commits to the collected values by inflicting those values to base station, it cannot change any of the collected values.

The authors in [18] in addition assume that each detector node options a novel image and shares a separate secret scientific discipline key with the bottom station and with the collector. These keys alter data confidentiality, integrity and authentication. In [4], detector nodes use the scientific discipline algorithms only if a cheating activity is detected. A topological constraint square measure introduced to form a secure aggregation tree (SAT) that facilitates the observance of data aggregators. In SAT, any kid node is in a very position to listen to the incoming data of its parent node. Once the combination data of a data soul is questionable, a weighted vote theme is utilized to work out whether or not or not the information collector is properly behaving or is cheating. If the information collector could also be a misbehaving node, then Sabbatum is fixed domestically therefore the misbehaving data collector is excluded from the aggregation tree. SecureDAV protocol [15] is implausibly like [18] except that elliptic curve cryptography is utilized for cryptography functions. Moreover, SecureDAV improves the data integrity vulnerability by language the combination information. SecureDAV could be a clustered approach where all detector nodes among a cluster share a secret cluster key.

Each detector node is in a very position to get a partial signature over the combination data. Every data collector aggregates its cluster data and broadcasts the combination data to its cluster. Each detector node within the cluster compares its data with the combination data broadcasted by the information collector. A detector node half signs the combination data if and on condition that the excellence between its data and aggregate data could be a smaller quantity than a threshold. Finally, the data soul combines the partial signatures to make a full signature of the combination information and sends it to the bottom station. SecureDAV provides data confidentiality, knowledge integrity, and supply authentication. However, the theme incurs high communication overhead on data validation and supports entirely the common aggregation operates.

In [11], a Secure Hop-by-hop data Aggregation Protocol (SDAP) is projected. The authors of SDAP square measure driven by the actual fact that compared to low-level detector nodes; additional trust is placed on the high-level nodes (i.e., nodes nearer to the root) throughout a conventional hop-by-hop aggregation technique in a very tree topology. As a result of combination data calculated by a high-level node represents the information of an outsized range of low-level detector nodes. If a compromised node is nearer to the bottom station, the false combination data created by this compromised node will have an even bigger impact on the last word result computed by the bottom station. Since all detector nodes have easy hardware that is in danger of compromise, none of those low cost detector nodes need to be plenty of trustable than others. Hence, SDAP aims to chop back the approach of reducing the trust on high-level nodes by following the divide-and-conquer principle. SDAP dynamically partitions the topology tree into multiple logical groups (sub trees) of comparable sizes using a probabilistic approach. throughout this approach, fewer nodes square measure set below a high-level detector node in a very logical sub tree resulting in reduced potential security threat by a compromised high-level node. SDAP provides data confidentiality, supply authentication, and data integrity. In [9], the authors argue that compromised nodes have access to cryptographically keys that square measure accustomed secure the aggregation technique then cryptographically primitives alone cannot provide a good enough resolution to secure data aggregation draw back.

Supported this observation, the authors propose a Secure and rELiable data Aggregation protocol, mentioned as SELDA that produces use of an online of trust. The elemental arrange behind SELDA is that detector nodes observe actions of their near nodes to develop trust levels (trustworthiness) for every the atmosphere and therefore the near nodes. Detector nodes use observance mechanisms to note node convenience, sensing and routing, misbehavers of their neighbors. These misbehaviors square measure quantified as trust levels exploitation Beta distribution performs [14, 23]. Detector nodes exchange their trust levels with near nodes to form an online of trust that allows them to examine secure and reliable methods to data aggregators. Moreover, to spice up the responsibility of the mass data, data aggregators weigh detector knowledge they receive exploitation the online of trust. One important property of SELDA is that, as a result of the observance mechanisms in use, it will notice if data human is below DoS attack.

The simulation results show that SELDA can increase the responsibility of the mass data at the expense of a tolerable communication overhead. In [13], the authors improved the foremost arrange of SELDA by introducing useful name thought where each helpful name price is computed over detector node actions with relevancy that perform. Hence, security of data aggregation method is ensured by selecting certain data aggregator's victimization aggregation helpful name and by constant detector information exploitation sensing helpful name. The simulation results show that exploitation helpful name is more practical than exploitation general name once evaluating the attribute of a detector node. In wireless sensor networks, a compromised detector node can inject false data throughout data forwarding and aggregation to forge the integrity of mass data. It's extremely fascinating for detector nodes to note and drop false knowledge as shortly as getable thus on avoid depleting their restricted resources like battery power and data live [7]. although several secure data aggregation protocols [15], 18],[19] square measure able to notice the false data injected by detector nodes, false data injections by compromised data aggregators can't be detected by these ways in which.

The explanation is that data aggregation winds up in data alterations and thus a modification in mass data as a result of false data injection is extremely arduous to note. Such false data injections by compromised data aggregators

can merely finish in false alarms that waste the network's resources and deflate the operational efficiency [7]. Recently, some work has been reported on detection of false data injections throughout knowledge aggregation so as that the warning among the network is reduced [5]-[7]. In [5], [6] secure data aggregation drawback is addressed from intrusion detection perspective. Among the projected theme, associate Extended Kalman Filter (EKF) based mechanism to note false injected data is projected. Alongside the utilization of EKF, the projected mechanism monitors detector nodes to predict their future real in-network mass values. For mass values, a typical vary is decided to note false data injections. Exploitation utterly completely different aggregation functions (average, sum, max, and min), the authors show the simplest way to accumulate ancient ranges on paper. Moreover, it's in addition shown that the projected EKF is employed to supply effective native detection mechanisms. The created native detection approaches square measure able to differentiate between malicious events and emergency events and thus it will deflate the warning rate among the network. in depth simulations square measure performed to determine performance of native detection mechanisms, at the side of false positive rate and detection rate, beneath utterly completely different aggregation functions. Simulation results demonstrate that the projected techniques bring home the bacon fascinating performance to watch false injected data. The work given in [7] realizes the actual fact that many existing false knowledge detection techniques ponder false data injections throughout data forwarding entirely.

The paper presents a knowledge aggregation and authentication protocol, called DAA, to integrate false data detection with data aggregation and confidentiality. To support data aggregation on with false data detection, a observance algorithmic rule is projected. Victimization these observance algorithms, the observance nodes of every data individual put together conduct data aggregation and figure the corresponding small-size message authentication codes for data verification at their try mates. To support confidential data transmission, the detector nodes between two consecutive data aggregators verify the data integrity on the encrypted knowledge rather than the plain knowledge. Each data packet is appended with a pair of life-size message authentication codes, each consisting of T+1 small-size message authentication codes. Performance analysis shows that DAA detects any false data injected by up to T compromised nodes, that the detected false knowledge do not appear to be forwarded on the so much facet enchant data individual on the trail. Despite that false data detection and data confidentiality increase the communication overhead, simulation results show that DAA can still deflate the amount of transmitted data by up to hour with the help of data aggregation and early detection and dropping of false knowledge.

The authors of [8] address the simplest way to verify a warning threshold dynamically and efficiently thus on minimize the warning chance in a very wireless detector networks deployed in realistic environments. Among the projected dynamic threshold theme, the brink changes in accordance with the warning rate. Hence, a stronger detection chance and reduced form of false alarms square measure achieved. Considering the realistic preparation eventualities, the paper proposes to chop back the impact of noise by taking a weighted average of assorted sensing units' readings for a similar target. The paper takes advantage of the actual fact that sensing units of assorted kinds square measure affected at varied degrees by the environmental factors. The authors put together propose Associate in nursing data aggregation algorithm to work out the detection chance of a target by fusing knowledge from multiple sensors. Although data confidentiality and authentication do not appear to be thought-about among the projected data aggregation algorithmic rule, the simulation results show that it improves the target detection accuracy and minimize warning rate among the network. All of the on high of secure data protocols use actual detector knowledge for aggregation and thence would like cryptography of detector knowledge at aggregators. However, the protocols projected in [12], [16] don't need actual data then they are able to integrate security and data aggregation seamlessly. In [12], the author's gift Energy economical and Secure Pattern primarily based knowledge Aggregation (ESPDA) protocol that considers every data aggregation and security ideas on in cluster-based wireless detector networks. ESPDA is that the initial protocol to accept data aggregation techniques while not compromising security. ESPDA uses pattern codes to perform data aggregation. The pattern codes square measure representative data things that square measure extracted from the particular data in such the best means that every pattern code has sure characteristics of the corresponding actual data.

The extraction technique might vary wishing on the kind of the actual data. As an example, once the actual data square measure pictures of kinsmen perceived by the police work sensors, the key parameter values for the face and body recognition square measure thought-about as a result of the representative data looking forward to the applying requirements. Once, a detector node consists of multiple sensing units' pattern codes of the detector node square measure obtained by combining pattern codes of the individual sensing units. Instead of transmittal the complete perceived data, detector nodes initial generate then send the pattern codes to cluster heads. Cluster heads verify the distinct pattern codes then request entirely one detector node to send the actual data for each distinct pattern code. This approach makes ESPDA each energy and information measure economical. ESPDA is in addition secure as results of cluster heads do not have to rewrite the data for knowledge aggregation and no encryption/decryption secret is broadcast. in addition, the projected no interference OVSF (Orthogonal Variable Spreading Factor) block hopping technique additional improves the security of ESPDA by randomly dynamic the mapping of data blocks to NOVSF time slots. In [16], Secure Reference-Based knowledge Aggregation (SRDA) protocol is projected for cluster-based wireless detector networks. Like ESPDA, SRDA put together realizes the actual fact that knowledge aggregation protocols need to add conjunction with the data communication security protocols, which any conflict between these protocols may turn out loopholes in-network security like violating data confidentiality. In SRDA, knowledge perceived by detector nodes square measure compared with reference data values then entirely the excellence knowledge square measure transmitted.

Reference data is taken as a result of the typical price of form of previous detector readings. The motivation behind

SRDA is that it is crucial to chop back the quantity of bits in an exceedingly transmission as a results of radio communication is that the most energy-consuming activity in a very detector node. Whereas data aggregation reduces the number of packets, decreasing the scale of the transmitted packets will additional improve the energy savings. In commonplace data aggregation algorithms, sensors transmit their raw perceived knowledge to the cluster heads. This wastes energy and data live since a particular varies of the data might keep an equivalent in each packet. However, SRDA transmits the differential knowledge rather than the raw perceived data. That is, the raw knowledge perceived by detector nodes square measure compared with reference data then entirely the excellence data is transmitted. As example, let 102º F denote the temperature measure of a detector node. If 100º F is taken into consideration as reference temperature by the cluster head, the detector node will send entirely the excellence (i.e., 2º F) of the current discharge from the reference price among the transmission. Consequently, differential aggregation has nice potential to scale back the amount of data to be transmitted from detector nodes to cluster heads. The cringe of ESPDA [12] and SRDA [16] is that they're doing not allow intermediate nodes to perform data aggregation. That is, detector data are mass entirely at the immediate data someone that considerably limits the great issue concerning data aggregation.

V. CONCLUSION

This paper provides a close review of secure knowledge aggregation conception in wireless sensor networks. To offer the motivation behind secure knowledge aggregation, first, the protection necessities of wireless device networks are bestowed and therefore the relationships between knowledge aggregation conception and these security necessities are explained. An intensive literature survey is bestowed by summarizing the progressive knowledge aggregation protocols.

VI. REFERENCES

[1] S. Ozdemir, Yang Xiao, Secure data aggregation in wireless sensor networks: Acomprehensive overview, in: Computer Networks 53 Elsevier (2009) 2022–2037.

[2] J. Yick, B. Mukherjee, D. Ghosal, Wireless sensor network survey,Comput. Networks 52 (12) (2008) 2292–2330.

[3] K. Akkaya, M. Demirbas, R.S. Aygun, The Impact of Data Aggregation on the Performance of Wireless Sensor Networks, Wiley Wireless Commun. Mobile Comput. (WCMC) J. 8 (2008) 171–193.

[4] K. Wu, D. Dreef, B. Sun, Y. Xiao, Secure data aggregation without persistent cryptographic operations in wireless sensor networks, AdHoc Networks 5 (1) (2007) 100–111.

[5] B. Sun, X. Jin, K. Wu, Y. Xiao, Integration of secure in-network aggregation and system monitoring for wireless sensor networks, in: Proceedings of IEEE International Conference on Communications (IEEE ICC'07), 2007, pp. 1466–1471.

[6] B. Sun, N. Chand, K. Wu, Y. Xiao, Change-point monitoring for secure in-network aggregation in wireless sensor networks, in: Proceedings of IEEE Global Telecommunications Conference, IEEE GLOBECOM, 2007, pp. 936–940.

[7] H. Çam, S. Ozdemir, False data detection and secure data aggregation in wireless sensor networks, in: Yang Xiao (Ed.), Security in Distributed Grid Mobile and Pervasive Computing, Auerbach Publications, CRC Press, 2007.

[8] B. Parekh, H. Çam, Minimizing false alarms on intrusion detection for wireless sensor networks in realistic environments, in:Proceedings of IEEE Military Communications Conference, 2007, pp. 1–7.

[9] S. Ozdemir, Secure and reliable data aggregation for wireless sensor networks, in: H. Ichikawa et al. (Eds.), LNCS 4836, 2007, pp. 102–109.

[10] R. Rajagopalan, P.K. Varshney, Data aggregation techniques in sensor networks: a survey, IEEE Commun. Surveys Tutorials 8 (4)(2006).

[11] Y. Yang, X. Wang, S. Zhu, G. Cao, SDAP: a secure hop-by-hop data aggregation protocol for sensor networks, in: Proceedings of the ACM MOBIHOC'06, 2006.

[12] H. Çam, S. Ozdemir, P. Nair, D. Muthuavinashiappan, H.O. Sanli,Energy-efficient and secure pattern based data aggregation for wireless sensor networks, Comput. Commun., Elsevier 29 (4)(2006) 446–455.

[13] S. Ozdemir, Functional reputation based reliable data aggregation and transmission for wireless sensor networks, Elsevier Comput.Commun. 31 (17) (2005) 3941–3953

[14] S. Ganeriwal, M.B. Srivastava, Reputation-based framework for high integrity sensor networks, in: Proceedings of the Second ACM Workshop on Security of Ad Hoc and Sensor Networks, Washington DC, 2004, pp. 66–77.

[15] A. Mahimkar, T.S. Rappaport, SecureDAV: a secure data aggregation and verification protocol for wireless sensor networks, in:Proceedings of the 47th IEEE Global Telecommunications Conference (Globecom), November 29–December 3, Dallas, TX,2004.

[16] H.O. Sanli, S. Ozdemir, H. Çam, SRDA: secure reference-based data aggregation protocol for wireless sensor networks, in: Proceedings of the IEEE VTC Fall Conference, Los Angeles, CA, 26–29 September 2004, pp. 4650–4654.

[17] J. Newsome, E. Shi, D. Song, A. Perrig, The Sybil attack in sensor networks: analysis and defenses, in: Proceedings of the Third IEEE/ACM Information Processing in Sensor Networks (IPSN'04), 2004, pp.259–268.

[18] B. Przydatek, D. Song, A. Perrig, SIA: secure information aggregation in sensor networks, in: Proceedings of SenSys'03, 2003, pp. 255–265.

[19] W. Du, J. Deng, Y.S. Han, P.K. Varshney, A witness-based approach for data fusion assurance in wireless sensor networks, in: Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '03), 2003, pp. 1435–1439.

[20] L. Hu, D. Evans, Secure aggregation for wireless networks, in:Proceedings of the Workshop on Security and Assurance in Ad Hoc Networks, Orlando, FL, 28 January 2003.

[21] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, A survey on sensor networks, IEEE Commun. Mag. 40 (8) (2002) 102–114.

[22] A. Perrig, R. Szewczyk, D. Tygar, V. Wen, D. Culler, SPINS: security protocols for sensor networks, Wireless Networks J. (WINE) 2 (5) (2002) 521–534.

[23] A. Josang, R. Ismail, The beta reputation system, in: Proceedings of the 15th Bled Conference Electronic Commerce, 2002.

[24] Crossbow Technologies Inc. <http: //www. xbow.com>.