Ensuring reliability and freshness for Data Aggregation in Wireless Sensor Networks

Shehzad Ashraf Ch., Mian Muhammad Omair, Iftikhar Ali Khan and Tahir Afzal Malik

***Abstract*—The emergence of senor node architecture with its advance capabilities to control the different hardware units and its enhancements in low power and affordable computational devices has made sensor networks from dream to reality. Sensor networks are deployed in widespread targeted areas where they can work for many years and can sense the environment behavior and its different variables without any need to externally charge their installed batteries, the security in sensor networks has become most important aspect along with low power, as the sensors are unattended so there is more possibility of attack in WSN than usual computer networks. Data aggregation security is an important task as if some false node injects a highly odd data values it will highly effect the whole aggregation process. The paper reviews the need of security for data aggregation and propose an architecture which eliminates the false values injection as well as it provides end to end reliability and data freshness, the architecture is also energy optimized.**

***Index Terms*— data aggregation, sensor networks, energy efficiency, Hash.**

I. Introduction

Wireless sensor networks are normally unattended and self configurable networks, which are composed of a few to thousands of lightweight and portable tiny sensing nodes. These networks are deployed in remote and hostile environments where these nodes can sense temperature, pressure, vibration, motion, sound and even the pollutant levels in targeted regions [2]-[9]. When the sensor node senses some behavior or phenomenon from the environment, transducer generates the signal for the sense data which is further processed and store by the installed microprocessor and after processing the signal, transceiver transmits this data to base station or some upper level aggregator node, through which the sensor node is wirelessly connected. Performing all this complex functionality, the size of the sensor node just vary from a shoebox to a dust of grain [3]. As the sensor nodes are normally targeted in an uncontrolled environments, physical approaching to deployed sensors is not possible, so the sensor nodes have the built in self configuration functionality. Sensor nodes make use of multi hop routing algorithms, through which multiple sensing nodes simultaneously send the data to some other nodes or base station.

Wireless sensor networks can use infrared or laser light, but these technologies require clear line of sight. So wireless sensor networks use radio communication technology for communication purpose, which does not require any clear line of sight [3]. The sense data from the leaf nodes is routed through multiple routing paths and intermediate nodes and at the end it reaches to a base station. The base station may be a simply a computer or some specialized hardware which can perform some computation on it, store and forward data and can also respond to the data sending nodes.

The emergence of senor node architecture with its advance capabilities to control the different hardware units and its enhancements in low power and affordable computational devices has made sensor networks from dream to reality. Sensor networks are deployed in widespread targeted areas where they can work for many years and can sense the environment behavior and its different variables without any need to externally charge their installed batteries. Early sensor networks were used only for military purposes such as in battlefield surveillance and keeping track the motion and other different activities of the enemy in remote and unreachable areas. Due to the recent developments and enhancements in sensor networks technology, wireless sensor networks are not now merely limited to military applications.

Its typical applications are habitat monitoring, object tracking, remote controlling, traffic monitoring [4] and its most complex and mission critical application is to monitor and control the nuclear reactors and making preemptive actions in case of any problem occurs during its normal working functionality [5].

Wireless sensor networks are resource limited networks which have low energy with less communication and computation. From the energy consumption point of view communication is the most costly process in wireless sensor networks [1,25].In wireless sensor networks, wireless medium is used for data transfer from source to destination, so the security is the prime factor that should be considered during the transmission of data, because anybody tuned to that particular frequency gain access to the sensed data [6]. Wireless sensor networks are normally deployed in unattended, untrusted and hostile environments where the sensor nodes and wireless communication links can be eavesdropped easily. Adversary by compromising only one sensor node or a single wireless link can easily forge or alter the data [7]. Sensor nodes have limited computational power, small memory size and low storage capacity as compared to other networks so during the design of any security and routing protocol for wireless sensor networks, the resource limitation factor is always considered. Specially the energy is

Manuscript received January 5, 2011. This work was supported in part by the Al-Faisal University Abha Kingdom of Saudi.

Mr. Shehzad Ashraf, Mian Muhammad Omair and Iftikhar Ali Khan are with department of computer science International Islamic University Islamabad, Pakistan, Tahir Afzal Malik is With Al-Faisal University Abha Kingdom of Saudi Arabia.

Email: t.a.malik@pscabha.edu.sa

the scarcest resource of the wireless sensor networks which is directly concerned with the life time of the senor node, so normal public/private key algorithms, which require complex mathematical computation are not feasible for these networks [9]. The security of wireless sensor networks is broadly categorized into two main types, internal security and external security. Internal security is called data privacy as well, and it is maintaining the privacy of sensed data from the trusted sensor nodes inside the network. The second type of security is called external security or data security, in which sensed data is protected from outsiders such as adversaries or eavesdroppers [7].

II. Application domain

Early sensor networks were used only for military purposes such as in battlefield surveillance and keeping track the motion and other different activities of the enemy in remote and unreachable areas. Due to the recent developments and enhancements in sensor technology, wireless sensor networks are not now merely limited to military applications.

Its typical applications are habitat monitoring, object tracking, remote controlling, traffic monitoring [4] and its most complex and mission critical applications are to monitor and control the nuclear reactors and making preemptive actions in case of any problem occurs during their normal working functionality [5].

In some specified environments, wireless sensors are used for fire detection and alarming purposes and can also be used to check the pollution level, traffic monitoring and enemy troops movement as well [6]. Some specific sensors can be used in patient's health care, where the sensors are used to measure the patient's blood pressure and his heart beat as well. In future, sensors will be used for data gathering related to the household details such as water usage, power consumption and assigning values to common trends and will be used for making some future predictions and recommendations as well [7].

III. Data Aggregation

Sensor nodes are deployed normally in remote and unattended environments where their maintenance and battery changing or charging is not possible, so saving the battery power of the sensor node increases the lifetime of the entire network. From energy perspective, communication is the most costly and expensive process in wireless sensor networks. Because of limitation of its design structure, sometimes it may possible that more than one sensor nodes have overlapping targeted regions which causes generation of redundant data packets. Data is correlated in terms of time and apace whenever it is sensed from the sensor nodes, so sending duplicate data values again and again may lead to expire sensor nodes early [8].

Data aggregation is performed at some intermediate sensor nodes for partially processing raw data and making sense data values more meaningful to high level sensors. Senor nodes sense and transmit raw data in seconds, so sending this raw data in bulk quantity causes energy blindness [7]. Whenever the child/leaf sensor nodes sense the data, they transmit their sense data to aggregator node, which then perform some aggregation function on this raw data and converts it into more meaningful format [10]. The most common aggregation operation is to calculate the average value for the sensed data [6]. For example when sensor nodes are deployed in region where they are required to sense the humidity or temperature of the surrounding environment for some specific period of time, after sensing they all will send their sense data to the intermediate aggregate node and aggregator node will transform this raw data into meaningful format by calculating its average and then sends this aggregated value to high level aggregator or base station if it is directly connected to it.

All the data from child nodes to the base station is traveled through intermediate aggregate nodes [10], so if the aggregator node is compromised, adversary will access all the data coming to the aggregator node. In some environments, the aggregator nodes are also acting as a cluster head, which stores all the keys of that particular cluster [11], so compromising only the cluster leader, the adversary gain access to all the secret keys stored. As data travels wirelessly in sensor networks so security of these sensing nodes and traveling data are now most favorite area for research purposes.

IV. Data Aggregation security in WSN

In wireless sensor networks, wireless medium is used for data transfer from source to destination, so the security is the prime factor that should be considered during the transmission of data, because anybody tuned to that particular frequency gain access to the sensed data [6]. Wireless sensor networks are normally deployed in unattended, untrusted and hostile environments where the sensor nodes and wireless communication links can be eavesdropped easily. Adversary by compromising only one sensor node or a wireless link can easily forge or alter the data [7]. Sensor nodes have limited computational power, small memory size and low storage capacity as compared to other networks so during the design of any security and routing protocol for wireless sensor networks, the resource limitation factor is always considered. Specially the energy is the scarcest resource of the wireless sensor networks which is directly concerned with the life time of the senor node, so normal public/private key algorithms, which require complex mathematical computation are not feasible for these networks [9]-[24]. The security of wireless sensor networks is broadly categorized into two main types, internal security and external security. Internal security is called data privacy as well, and it is maintaining the privacy of sensed data from the trusted sensor nodes inside the network. The second type of security is called external security or data security, in which sensed data is protected from outsiders such as adversaries or eavesdroppers [7].

In wireless sensor networks data from source to destination is transferred through some intermediate aggregator nodes and these nodes act like a dominating nodes. From security point of view these intermediate aggregation nodes hold the most critical position in wireless sensor networks. For example wireless sensor network is deployed in some temperature critical environment, which is divided into different zones and in each zone some sensor nodes are deployed and one of them acts like a aggregate cluster node.

In each zone of deployed environment, it is required to maintain the average temperature value to 25°C, and if the average temperature value in any zone is greater or lesser than 25°C, a temperature control system which is associated with base station begins to start working for maintaining the average temperature value. Leaf sensing nodes which are well equipped with some powerful security mechanism, after sensing the temperature value, perform some cryptographic function on it and send this cipher text to aggregate cluster node. Aggregate cluster node decrypts this cipher text into plain text, performs average aggregation function on the decrypted data and sends this aggregation value to the base station. If this trusted aggregate cluster node is compromised, the adversary can easily forge or alter the temperature values and disturb the whole temperature of the environment by sending fake and bogus aggregation results to temperature control system.

Providing a secure data aggregation, while preserving the security and privacy of the sense data is still challenging task because traditional security algorithms based on cryptography and public/private keys are very expensive and are not feasible in wireless sensor networks [9].

Depending on the encryption schemes, secure data aggregation protocols in wireless sensor networks are grouped into two main categorizes, Hop-by-Hop and End-to-End encryption protocols [7]. In hop-by-hop secure data aggregation, sensor nodes sense the data, encrypt it and then send this cipher text to the aggregator node, which then decrypts it, perform some data aggregation function on the received data from its child nodes and then again encrypts this aggregated data and sends it to the upper level node or base station. But in End-to-End secure data aggregation, the aggregation nodes do not have the decryption keys so data aggregation function at intermediate nodes is performed on the encrypted data [12]-[13].

V. Literature Review

Wireless sensor networks are emerging technologies currently being deployed in seismic monitoring, wild life studies, manufacturing and performance monitoring. These networks are densely deployed in some predetermined geographical area to self organize into ad-hoc wireless network together and aggregate data [16]. These networks are composed of tiny sensor nodes which are powered by a small built in batteries and are deployed in hostile and uncontrolled environments where these networks has to work for many years[1]. Because of their limitations in energy, storage capacity, computation and communication, these networks pose unique security challenges [2]. [1] Proposed a strong security architecture using network coding and the use of hash functions, the architecture is energy optimized , but the architecture can work only for single hop network, Our proposed architecture is an extension of [1] for multi hop networks.

Data aggregation can also reduce data packet size, number of data transmissions and the number of nodes involved to gather data [7]. So to save energy in sensor networks, data aggregation is put forward as an in-network processing, the data from source to destination is transferred through intermediate aggregator nodes, which perform aggregate function on the data and then sends aggregation results to a higher level aggregators [17]. As sensor networks use radio signals for communication purposes, anybody tuned to that particular frequency can forge or alter the data, so the confidentiality of the transmitted data can be considered as the most critical [6]-[7]. Confidentiality in wireless sensor networks is provided through Homomarphic encryption and allows network data aggregation. Homomarphic encryption provides the way to calculate the aggregate over the encrypted values. But Homomarphic encryption does not provide data integrity, so by using public key elliptic curve cryptography, digital signatures can be used to provide data integrity as well [6]. The sensed data is not only to be protected externally but from internal nodes as well. So privacy of sensor data is another security issue in sensor networks. For preserving the privacy of sensed data and hiding its details from the trusted nodes, the algorithm uses the additive property of complex numbers. Sensor node is pre-deployed with the two numbers, one is real private seed and other is imaginary private seed. When the sensor node sense the data, it first adds it with the real private seed and gets 'a' then again it adds the obtained 'a' with the imaginary private seed 'bi' and data is transformed into complex number form, encrypts complex number form by using symmetric key and then transmits this cipher text to its parent [7]. Data involved in aggregation purposes should not only belong to trusted nodes but also follow reliable links. Reputation values are used to ensure that the data sending nodes are trusted and are not compromised. The nodes and the aggregators can sense the behavior of the neighboring sensor nodes in the environment. Depending on the sense behavior of sensor nodes a reputation value is calculated, which depends on the sensor ability of sensing, routing and availability. This web of trust relationship provides secure and reliable path for data transfer from sensor to aggregate node [8].

[25] proposed a routing protocol that ensure that at least two sensing nodes share one common key with the probability of 1with low memory, communication overhead and less energy, In the proposed key distribution scheme the network topology is divided into one base station and many other substations or cluster heads. Main base station always remains online and sensor nodes are able to move from one location to another easily, thus changing its membership from one cluster head to another. So when the sensor nodes move from one cluster head to another it become very important for the base station and cluster head to ensure the authentication of the newly joining sensor and prevent the joining of malicious sensor. Sensor nodes are lack of memory capacity, so initially the sensor nodes are predeployed with some keys from a large key pool. Initially the traditional key discovery protocol is used to find the common key between the neighboring nodes. When the sensor node changes its location and wants to become the member of new cluster head, it first sends the request of the base station. The request

contains source and destination address, with base station, sensor node and router and also the MAC calculated on the random value and key shared between the base station and the sensor node. When the base station receives the message first it will check then authenticity of the sensor node by calculating and verifying it with the help of MAC, if the result is positive then the base station will generate a session key KNR for roaming sensor node and its newly cluster head. Then the base station will send the approval message to the cluster head. The format of message from base station to the cluster head would be like

appv = {Src=BS, Dst=RT, E(KBT, SN||R0||R1||KNR)}

When the cluster head receives the appv message from the base station, it will first decrypt the message with the shared key KBT with the nase station and extract the session key. Then the cluster head will calculate the MAC on the extracted session key and will send this MAC to the sensor node. When the sensor node receives the message, it will itself calculate the session key and then calculate the MAC on locally calculated session and then verifies it by comparing it with the received value of MAC. If the result is positive the authentication is completed and afterwards all the communication between sensor node and the router / cluster head is carried by using this newly calculated session key. As less hops involve in data transfer session so the communication over head is significantly decreased.

[26] proposed an efficient solution for secure data transfer in lossless many-to-one transmission in wireless sensor networks.Data from sensor nodes to base station is transferred through aggregate nodes which perform some aggregation function like sum, max, min and average. In this case only one value is sent to the base station which does not knows the exact value of each sensor. In the proposed scheme lossless secure data transmission scheme is used, which the BS cannot afford the loss of some information from its sensors. Base station is full fledge computer which has private key SKBS and its corresponding public key PKBS is shared among all the sensor nodes. Sensor nodes also share the secret key Ki with the base station. Initially the BS randomly generate a value V, signs it digitally using its private key and multicast this value to all the sensing nodes. When the leaf sensing node Ui receives digitally signed value, it first verifies the digital signatures and then it will locally calculate the pseudo random t bits (c1,c2,…..ct). Then again the sensing node Ui calculates the sequence of bits (d1,d2,……dt) such that the (b1,b2,……bt) be the binary representation of the symbol the sensor node want to transmit. It will be compared such a way that if (b1,…..,bt) = (c1,….,ct) then also (di,….,dt) = (b1,…..,bt)
Else (d1,….,dt) = (b1 xor c1,……bt xor ct).

Then the Ui node will calculate the pseudo random number σi as follows

σi lsbs (H(di,…,dt) // V// Ki)

The leaf node Ui then sends the pair(Ii, σ i) to its parent or to the BS if it is directly connected to it. If the parent node gets all of the expected pairs (Ij, σ j)j from its leaf nodes then it will calculate the I = Vj Ij (V is bit or operation) and σ = Σ j σi (mod 2S). If the current node is not the base station it will send the (I σ) to the upward parent node other wise this is final aggregate message. When the base station receives the pair, it will first calculate the binary representation (bi,1,….,bi,t) for each sensor Ui this is obtained from (di,1,….,di,t), that is generated previously from Ui and is contained in receive value of I. At the end of all this the base station will compute the pseudo random integer which is linked with (di,1,….,di,t), through which the integrity of whole aggregated message is computed.

[4] provided an efficient and secure routing and key management scheme for mobile sinks with very low communication overhead and energy consumption. The scheme consists of three phases: key predistribution, direct key establishment, and indirect key establishment.

Algorithms proposed for security purposes, focus on secure data transfer from source to destination, but at the same time it is also needed that proposed algorithm sure to decrease the communication overhead by transferring less number of bits through network. Secure End-to-End data aggregation protocol uses the additive homomarphic encryption and performs its functionality by calculating the aggregation value from cipher text received from the leaf sensing nodes. This protocol is basically proposed to decrease the transmission of extra bits for the nodes that are not participating in the aggregation. The nodes that are not responding or have no data values for sending, use "0" as their sense value and sends this cipher text to the aggregate node. One variable is used for keeping track the quantity of the non responding nodes [10].

The security issues such as authentication, integrity and data freshness become very crucial when sensors are deployed in hostile environments where they are prone to node failures and compromised [9]. Secure data aggregation (SDA) scheme is resilient to intruder devices and single node compromise. It is based on delayed aggregation and delayed authentication. Senor nodes need to buffer the data to authenticate it once the shared key is revealed by the base station. It also provides integrity and data freshness but data can be altered once the parent and child hierarchy is compromised [18]. Authentication can be provided both for end to end and hop by hop. For this purpose a pair of aggregated values is used, one is for authentication of hop-by-hop and the other one is for authentication of end-to-end. Besides such a pair, the ID list representing sensor nodes involves in a pair of aggregated values is produced and used to regenerate MAC to check integrity along the way at the base station. However, the concatenation of IDs will occur the overhead of data aggregation, particularly in scalability [19]. Node compromise in data aggregation is threatening as compromised sensing nodes will inject false data in aggregation. Injected false data and adversary node is identified by specified external nodes in parent child network hierarchy. The role of the external node is just to monitor the parent and children nodes and then report to the base station. Keys are predeployed and shared among nodes for authentication purpose and the judgment of false data nodes is done through decision of majority [20].

Wireless Sensor Networks are deployed normally in unattended mission critical environments, where the sensing nodes use the wireless media like electromagnetic radio signals for sending the data. Sensor nodes are not equipped with any costly temper red resistant hardware so they can be easily compromised and adversary can inject, alter, delete and change the order of the message and also compromises the trustworthiness of the information [2]. For example nodes are deployed to sense environment temperature. After sensing the nodes send the normal temperature 35 ~ 40 to the aggregate node, which then aggregates it by calculating average and sends the resultant aggregate value to the base station. During communication adversary injects some false node in the network or compromise some trusted nodes and sends odd data value such as 110 to the aggregator node, which when aggregates this odd value with the other true sensing values and sends the aggregation value to the base station. This false value will highly affect the final average aggregation result.

Adversary cannot only compromise the trusted sensor nodes but also can use laptop type devices that have strong computation and communication power with unlimited memory and battery life time. It may also possible that more than one nodes are compromised in the sensor network and these compromised nodes can also communicate and share hacked cryptographic information with each other via out of band channels.

It may possible that sensing node is compromised in such a way that it is replaying same data values again and again, to misguide the aggregation results, sending value is neither odd nor it is out of range.

Whatever the case is, sensor networks should be secured enough so that the adversary neither compromise the trusted senor nodes nor can inject false data values in aggregation phase. A proper security mechanism should be developed that identifies the false injected data and provides data freshness in data aggregation with low communication overhead.

VI. Proposed Architecture

Here we will propose a security mechanism in which first odd data values are identified and then the fault or compromised nodes are permanently removed from the network through hash base authentication at aggregate node.

The proposed architecture is shown in Figure 1. Initially the value P_0 is predeployed in all the sensor nodes and this value is shared with the aggregator node as well. When the leaf sensing node A senses some data A_1 from the environment, it concatenates A_1 with predeployed P_0 and calculates hash on it, and this calculated hash and the sense data A_1 is sent to next sensing node B.

The format of the data from the node A to B is like

$$\mathbf{A_1 // H (A_1 // P_0)}$$

When the sensing node B receives the data from the node A, it first calculates the difference of B_1 and A_1 like (B_1-A_1), and then concatenates it with the predeployed P_0, calculates its hash like H (B_1-A_1 // P_0), and appends the difference of B_1 and A_1 and calculated hash with the old data packet received from the sensor node A, and sends this data to the next sensing node C.

The format of the data packet from node B to C will be like

$$\mathbf{(A_1 // H (A_1 // P_0)) // (B_1-A_1 // H (B_1-A_1 // P_0))}$$

When the data is reached at the node C, it then calculates the difference of C1 and A1 (C1-A1) by using network coding and also concatenates C1-A1 with P0, calculates it hash and appends it with the packet received from the node B. The format of the data packet from node C to D will be like this.

$$\mathbf{(A_1 // H (A_1 // P_0)) // (B_1-A_1 // H (B_1-A_1 // P_0)) // (C_1-A_1 // H (C_1-A_1 // P_0))}$$

The proposed architecture is shown in figure 1.

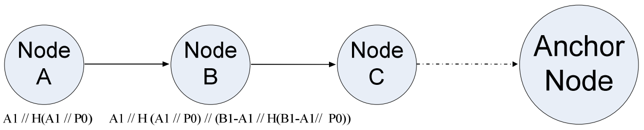

Figure 1: Block diagram of the overall scheme presented, in which three sensor nodes A, B and C are connected to each other and are transmitting the sensed data and calculated hash to the anchor node.

At the end the data will reached to the aggregate node. Aggregate node will first check the received readings of sensor nodes, if the values lie in some acceptable range, then it will calculate hash on it and compare it with the received hash. If the result is same the received values will be included in the final aggregation.

As the aggregate node will again calculate the hash function on the received data values so it can easily detect odd / false data values and will not include it in the aggregation.

Next time each node will use the H (A1 // P0) as a value of P1, as this value is changed in each session of communication so data freshness is maintained and there is no need to transmit the value of P again and again to all the sensor nodes which will cause communication overhead over head, as only difference of the sensed values is sent to the aggregate nodes so less number of bits are used so communication overhead is decreased.

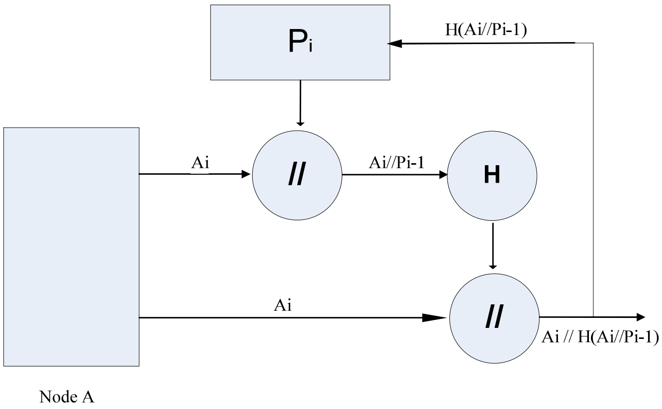

Figure 2: Block Diagram of Initiating Node A

Node A will first concatenate its sense value with the current value of P and then it will calculate the hash on it. After this node A will concatenate the hash code generated with its original sense value and transmit it to the next hop node B.

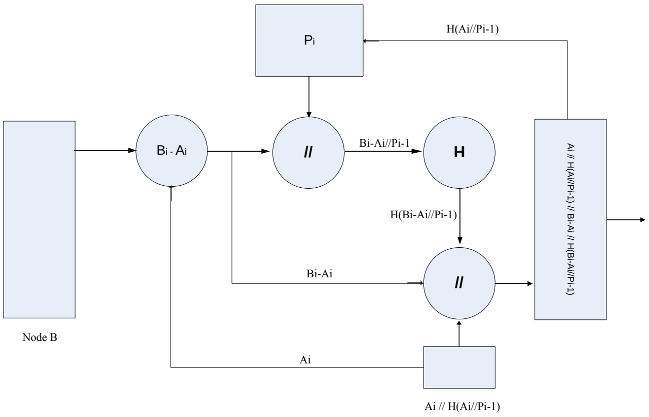

Figure 3: Diagram of Intermediate nodes

When the sensor node B gets the data from node A, it calculates the difference of its sense data and the sense data of node A, the difference is then concatenated with the current value of P and then hash is calculated on it. After this the difference of sense data between node B and node A, hash code generated and the data received from the previous node is transmitted to the next hop node, or to the anchor node if it is directly connected to it.

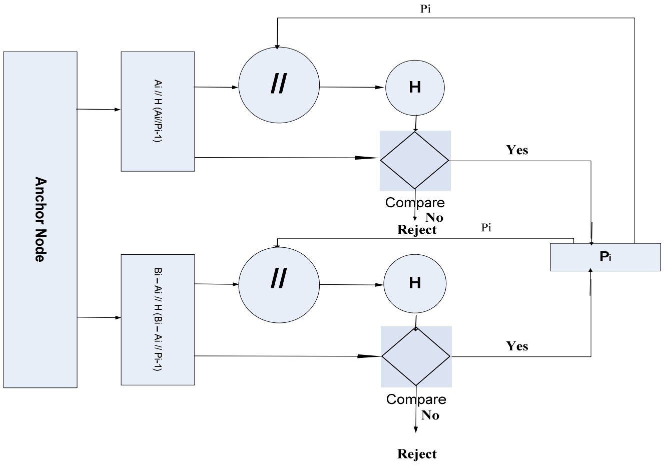

Figure 4: Anchor Node block diagram

When the anchor node gets the data from its child nodes, say nodes A and B, it first calculates the hash by concatenating the received plaintext values with value of P. Anchor node separately calculates the hash code for every sensor reading. After calculating the hash function, the anchor node will compare the calculated hash values with the hash values received from the leaf sensing nodes, if both received and calculated hash values are same then the received data is reliable. At the end of each successful communication session, the anchor node will update the value of P and will also broad cost this value to all the leaf sensing nodes to ensure the data freshness in each data communication session.

VII. Discussion

We have modified the single hop approach defined in [1], and ensured reliability of data in multi hop environment and detection of false data values and data freshness as well. As we are sending only reference based values which causes less transmission of bits and decreasing the communication overhead.

The scheme presented in [21], at the start of each communication session the leaf sensing nodes have to send their original sensing values to the cluster head which then calculates the reference value and then transmits the reference value back to the leaf sensing nodes. At the end of each communication session this reference value is erased from the memory of sensing nodes causes wastage of network resources. If the sensing node is compromised and sends the fake or replaying messages, there is no any mechanism provided to ensure freshness and dynamicity of the data. In our proposed scheme reliability and data freshness in aggregation is ensured and for decreasing the communication overhead reference based values transmission is used but no reference values are sent and erased at the start and end of each communication session. Although the scheme proposed in [22] is very efficient and reliable for maintaining confidentiality in data aggregation and detection of false data values. But it poses extra communication overhead, as in the first stage sensor nodes send the hash calculated on their sense value H(Vi) and in the second stage of data communication session nodes send the encrypted data value Enc(Vi)ki to the aggregator node. The scheme provided in [23], is an efficient technique for providing data confidentiality, authenticity and data freshness as well. As in this scheme packet based key is used which is linear combination of previous key and previous packet, so in noisy environments where the packet loss is very high, this scheme cannot work so efficiently because loss of only one packet will not only be the loss of that packet but also the loss of key for next packet.

VIII. Conclusion

Securing the data aggregation in wireless sensor is very important for accuracy sensitive applications like surveillance systems etc. We have proposed a network coding based architecture for providing security for data aggregation, the architecture provides end to end reliability without the use of acknowledgements, and the architecture can work in noisy and malicious environments.

Acknowledgment

The authors would like to thanks Mr. Syed Husnain Abbas Naqvi, Mr. Waqas Nasar and Mr. Zahid Mehmood for their valuable comments and suggestions.

References

[1] Shehzad Ashraf Ch, Zahid Mehmood, Rashid Amin, Dr. Mohammad Alghobiri, Tahir Afzal Malik "Ensuring Reliability & Freshness in Wireless Sensor Networks" 2010 International Conference on Intelligent Network and Computing (ICINC 2010)

[2] Tanveer Zia and Albert Zomaya "Security Issues in Wireless Sensor Netwoks"

[3] Kay Romer and Friedemann Mattern "The Design Space of Wireless Sensor Networks" NCCR-MICS, grant no. 5005-67322. IEEE Wireless Communicationss, Dec. 2004

[4] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, and J. Anderson, "Wireless Sensor Networks for Habitat Monitoring," *WSNA'02,* Atlanta, Georgia, September 2002

[5] N. Xu, S. Rangwala, K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, and D. Estrin, "A Wireless Sensor Network for Structural Monitoring," in Proceedings of the ACM Conference on Embedded Networked Sensor Systems, Baltimore, MD, November 2004.

[6] Julia Albath and Sanjay Madria "Secure Hierarchical Data Aggregation in Wireless Sensor Networks" IEEE Communications Society subject matter experts for publication in the WCNC 2009 proceedings.

[7] Rabindra Bista, Kyoung-Jin Jo and Jae-Woo Chang "A New Approach to Secure Aggregation of Private Data in Wireless Sensor Networks" 2009 Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing

[8] Suat Ozdemir "Secure and Reliable Data Aggregation for Wireless Sensor Networks"H. Ichikawa et al. (Eds.): UCS 2007, LNCS 4836, pp. 102–109, 2007.Springer-Verlag Berlin Heidelberg 2007.

[9] Hani Alzaid, Ernest Foo, Juan Gonzalez Nieto "Secure Data Aggregation in Wireless Sensor Networks: a survey" 6th Australasian Information Security Conference (AISC 2008), Wollongong, Australia, 2008

[10] A.S.Poornima and B.B.Amberker "SEEDA : Secure End-to-End Data Aggregation in Wireless Sensor Networks" 978-1-4244-7202-4/10/©2010 IEEE.

[11] Tanveer Zia and Albert Zomaya "A Security Framework for Wireless Sensor Networks" IEEE Sensors Applications Symposium Houston, Texas USA, 7-9 February 2006

[12] C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor networks," in The Second Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2005, pp. 109–117.

[13] J. Girao, D. Westhoff, and M. Schneider, "CDA: Concealed Data Aggregation in Wireless Sensor Networks," 40th IEEE International Conference on Communications, May 2005

[14] J. M. Kahn, R. H. Katz, and K. S. J. Pister, "Next century challenges: mobile networking for smart dust," MobiCom 99: Proc. 5th ACM/IEEE Intl. Conf. on Mobile computing and networking, pp. 271–2781, 1999.

[15] A. Ephremides and B. Hajek, "Information theory and communication networks: an unconsummated union,"IEEE Trans.on Inform. Theory, vol. 44, no. 6, pp. 2416–2434, 1998

[16] N. Hu, Randy R. K. Smith and P. G. Bradford 'Security for Fixed Sensor Networks' Proceedings of the 42nd annual Southeast regional conference, ACM Press, 2004, NY, USA

[17] Ying Sang, Hong Shen 'Secure Data Aggregation in Wireless Sensor Networks' IEEE Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06) 0-7695-2736-1/06

[18] Hu, L. & Evans, D. (2003) 'Secure Aggregation for Wireless Networks' in 'SAINT Workshops', IEEE Computer Society, pp. 384-394

[19] E. Mlaih and S. A. Aly, "Secure Hop-by-Hop Aggregation of End-toEnd Concealed Data in Wireless Sensor Networks." IEEE INFOCOM Workshops, 2008, pp. 1-6.

[20] Anuparp Boonsongsrikul, Kyung-suk Lhee and ManPyo Hong 'Securing Data Aggregation against False Data Injection in Wireless Sensor Networks' ISBN 978-89-5519-146-2, Feb. 7-10. 2010 ICACT 2010

[21] H. Ozgur Sanli, Suat Ozdemir and Hasan Cam 'SRDA: Secure Reference-Based Data Aggregation Protocol for Wireless Sensor Networks'

[22] Li Hui, Zheng Yanfei, Chen Kefei, Wen Mi 'A Hash Based Secure Aggregation Protocol for Sensor Network' Proceedings of the 2006 IEEE International Conference on Mechatronics and Automation June 25 - 28, 2006, Luoyang, China

[23] J. Shaheen, D. Ostry, V. Sivaraman, S. Jha, 'Confidential and secure broadcast in wireless sensor networks' 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07)

[24] Shehzad A. Mian Omair, Iftikhar A.K., Tahir A.M., 'Secure data aggregation in wireless sensor networks' 3rd International conference on machine learning and computing 2011.

[25] Ying Qiu, Jianying Zhou, Joonsang Baek and Javier Lopez, Authentication and Key Establishment in Dynamic Wireless Sensor Networks (Sensors 2010, 10, 3718-3731; doi:10.3390 / s100403718)

[26] Alexandre Viejo, Josep Domingo-Ferrer, Francesc Seb´e and Jordi Castell`a-Roca, Secure Many-to-One Communications in Wireless Sensor Networks (Sensors 2009, 9, 5324-5338; doi:10.3390/s90705324)

[27] Le Xuan Hung, Ngo Trong Canh, Sungyoung Lee, Young-Koo Lee and Heejo Lee, An Energy-Efficient Secure Routing and Key Management Scheme for Mobile Sinks in Wireless Sensor Networks Using Deployment Knowledge (Sensors 2008, 8, 7753-7782; DOI: 10.3390/s8127753)

Mr. Shehzad Ashraf Ch. got his MS degree in Computer science from International Islamic University Islamabad. He is a Gold Medalist in MS, currently working as lecturer in Department of computer science, International Islamic University Islamabad, Pakistan Email: shahzad@iiu.edu.pk

Mr. Mian Muhammad Omair. is a graduate student at, International Islamic University Islamabad, Pakistan Email: mian_92u@yahoo.com

Mr. Iftikhan Ali Khan got his MS degree in Computer science from International Islamic University Islamabad, Currently he is working as Research Associate in Department of computer science, International Islamic University Islamabad, Pakistan.
Email: iftikhan.khan@iiu.edu.pk

Mr. Tahir A. Malik did BSC (Hons) Computer Science, MSC Software Engineering, MBA Management and MS MIS from University of Bradford, UK, Currently he is working as Lecturer in Department of Management Information Sciences, Prince Sultan College for Tourism and Business, Al-Faisal University, Abha, Kingdom of Saudi Arabia Email: t.a.malik@pscabha.edu.sa