ISSN: 2321-7782 (Online)
Volume 1, Issue 5, October 2013
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

Secure Encryption Technique with Keying Based Virtual Energy for Wireless Sensor Networks

S. P. Santoshkumar [1]
Assistant Professor
Department of Computer science and Engineering
SNS College of Technology
Coimbatore – India

C. B. Sivaparthipan[2]
Assistant Professor
Department of Computer science and Engineering
SNS College of Technology
Coimbatore – India

D. Prabakar[3]
Assistant Professor
Department of Computer science and Engineering
SNS College of Technology
Coimbatore – India

Dr. S. Karthik[4]
Dean Cum Professor
Department of Computer science and Engineering
SNS College of Technology
Coimbatore – India

Abstract: ***In order to provide secure and cost-efficient encryption and keying for wireless sensor networks, this paper introduce a Secure Encryption and keying based on virtual energy for wireless sensor networks (WSN). Since sensors are resource limited wireless devices and the communication cost is the most dominant factors in WSN, the propose system can save the energy of the sensors by monitoring the wireless spectrum where the unattended sensors can be reused efficiently and generating dynamic keys for rekeying to avoid stale keys. Here the sensed data is encoded with RC4 encryption mechanism. The key to the mechanism dynamically changes as a function of residual virtual energy of the sensor. The intermediate nodes along the path to the sink are able to verify the authenticity and integrity of the incoming packets using a predicted value of the key generated by the sender's virtual energy, thus requiring no need for specific rekeying messages. To protect the keys from the malicious outsiders, hashing function is being used. This scheme can eliminate the false injection of data into network and eliminate insider threads and providing dynamic paths.***

Keywords: WSN security, RC4 encryption, hashing, virtual energy.

I. INTRODUCTION

Sensor network technology has rapidly developed in recent years and will be used in a variety of environments. Accordingly, people will come to rely more on sensor networks. For example, in a battlefield scenario, sensors may be used to detect the location of enemy sniper fire or to detect harmful chemical agents before they reach troops. Research on WSN indicates that energy required for transmission is greater than the energy required for processing data. Due to this fact, many energy aware routing protocols have been introduced. The sensor networks work on a very small battery having very low energy. It is near to impossible to change the battery of a node once it is deployed. In most of the cases, nodes survive on the energy recharged with the help of photovoltaic or thermal conversion.

It is very important to provide authentic and accurate data to surrounding sensor nodes and to the sink to trigger time-critical responses Protocols should be resilient against false data injected into the network by malicious nodes. Otherwise, consequences for propagating false data or redundant data are costly, depleting limited network resources and wasting response efforts. To focusing the key management, there are two fundamental key management schemes for WSNs: static and dynamic. In static key management schemes, key management functions (i.e., key generation and distribution) are handled statically. That is, the sensors have a fixed number of keys loaded either prior to or shortly after network deployment. On the other hand,

dynamic key management schemes perform keying functions (rekeying) either periodically or on demand as needed by the network. The sensors dynamically exchange keys to communicate. Although dynamic schemes are more attack resilient than static ones, one significant disadvantage is that they increase the communication overhead due to keys being refreshed or redistributed from time to time in the network.

There are many reasons for key refreshment, including: updating keys after a key revocation has occurred, refreshing the key such that it does not become stale, or changing keys due to dynamic changes in the topology. In this paper, we seek to minimize the overhead associated with refreshing keys to avoid them becoming stale. Because the communication cost is the most dominant factor in a sensor's energy consumption, the message transmission cost for rekeying is an important issue in a WSN deployment (as analyzed in the next section). Furthermore, for certain WSN applications (e.g., military applications), it may be very important to minimize the number of messages to decrease the probability of detection if deployed in an enemy territory. That is, being less "chatty" intuitively decreases the number of opportunities for malicious entities to eavesdrop or intercept packets.

II. RELATED WORKS

Dynamic keying schemes go through the phase of rekeying either periodically or on demand as needed by the network to refresh the security of the system. With rekeying, the sensors dynamically exchange keys that are used for securing the communication. DEEF [2], is that in reality battery levels may fluctuate and the differences in battery levels across nodes may spur synchronization problems, which can cause packet drops. Ma's work [3] applies the same filtering concept at the sink and utilizes packets with multiple MACs appended. A work [4] proposed by Hyun and Kim uses relative location information to make the compromised data meaningless and to protect the data without cryptographic methods. In [5], using static pair wise keys and two MACs appended to the sensor reports, "an interleaved hop-by-hop authentication scheme for filtering of injected false data" was proposed by Zhu et al. to address both the insider and outsider threats.

Another crucial idea of this paper is the notion of sharing a dynamic cryptic credential (i.e., virtual energy) among the sensors. A similar approach was suggested inside the SPINS study [6] via the SNEP protocol. In particular, nodes share a secret counter when generating keys and it is updated for every new key. However, the SNEP protocol does not consider dropped packets in the network due to communication errors. Although another study, Minisec [7], recognizes this issue, the solution suggested by the study still increases the packet size by including some parts of a counter value into the packet structure. The following sections will address the related works briefly.

A. Dynamic energy-based encoding and filtering

H. Hou, C. Corbett, Y. Li, and R. Beyah proposed DEEF .In critical sensor deployments it is important to ensure the authenticity and integrity of sensed data. Further, one must ensure that false data injected into the network by malicious nodes is not perceived as accurate data. Here they present the Dynamic Energy-based Encoding and Filtering (DEEF)[2] framework to detect the injection of false data into a sensor network. DEEF requires that each sensed event report be encoded using a simple encoding scheme based on a keyed hash. The key to the hashing function dynamically changes as a function of the transient energy of the sensor, thus requiring no need for re-keying. Depending on the cost of transmission vs. computational cost of encoding, it may be important to remove data as quickly as possible. Accordingly, DEEF can provide authentication at the edge of the network or authentication inside of the sensor network. Depending on the optimal configuration, as the report is forwarded, each node along the way verifies the correctness of the encoding probabilistically and drops those that are invalid. They have evaluated DEEF's feasibility and performance through analysis. Their results show that DEEF, without incurring transmission overhead (increasing packet size), is able to eliminate 90% - 99% of false data injected from an outsider within 9 hops before it reaches the sink.

B. Statistical en-route filtering of injected false data in sensor networks

Fan Ye, Haiyun Luo and Songwu Lu proposed the "Statistical En-Route Filtering of Injected False Data in Sensor Networks" to detect and drop false reports during the forwarding process Assuming that the same event can be detected by multiple sensors, in SEF each of the detecting sensors generates a keyed message authentication code (MAC) and multiple MACs are attached to the event report. As the report is forwarded, each node along the way verifies the correctness of the MAC's probabilistically and drops those with invalid MACs. SEF exploits the network scale to filter out false reports through collective decision- making by multiple detecting nodes and collective false detection by multiple forwarding nodes. Authors have evaluated SEF's feasibility and performance through analysis, simulation, and implementation. Our results show that SEF can be implemented efficiently in sensor nodes as small as Mica2. It can drop up to 70% of bogus reports injected by a compromised node within five hops, and reduce energy consumption by 65% or more in many cases.

C. SPINS: Security Protocols for Sensor Networks

A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. Tygar proposed the SPIN, As sensor networks edge closer towards wide-spread deployment, security issues become a central concern. So far, much research has focused on making sensor networks feasible and useful, and has not concentrated on security. They present a suite of security building blocks optimized for resource constrained environments and wireless communication. SPINS has two secure building blocks: SNEP and _TESLA. SNEP provides the following important baseline security primitives: Data confidentiality, two-party data authentication, and data freshness. A particularly hard problem is to provide efficient broadcast authentication, which is an important mechanism for sensor networks. _TESLA is a new protocol which provides authenticated broadcast for severely resource-constrained environments. They implemented the above protocols, and show that they are practical even on minimal hardware: the performance of the protocol suite easily matches the data rate of our network. Additionally, They demonstrate that the suite can be used for building higher level protocols.

D. Dynamic en-route scheme for filtering false data injection

Zhen Yu and Yong Guan proposed a dynamic en-route filtering scheme for false data injection attacks in wireless sensor networks. In sensor networks, adversaries can inject false data reports containing bogus sensor readings or nonexistent events from compromised nodes. Such attacks may not only cause false alarms, but also drain out the limited energy of sensor nodes. Several existing schemes for filtering false reports either cannot deal with dynamic topology of sensor networks or have limited filtering capacity. In our scheme, a legitimate report is endorsed by multiple sensing nodes using their own authentication keys generated from one-way hash chains. Cluster head uses Hill Climbing approach to disseminate the authentication keys of sensing nodes to the forwarding nodes along multiple paths toward the base station.

The purpose system will provide fulfill all issues discussed in the previous works and provide security in a efficient manner.

III. Overview of the System

In this paper provides secure communication framework provides a technique to verify data in line and drop false packets from malicious nodes, thus maintaining the health of the sensor network. It dynamically updates keys without exchanging messages for key renewals and embeds integrity into packets as opposed to enlarging the packet by appending message authentication codes (MACs). Specifically, each sensed data is protected using a simple encoding scheme based on a permutation code generated with the RC4 encryption scheme and sent towards the sink. The key to the encryption scheme dynamically changes as function of the residual virtual energy of the sensor, thus requiring no need for rekeying. The nodes forwarding the data along the path to the sink are able to verify the authenticity and integrity of the data and to provide non-repudiation.

The contributions of this paper are as follows. First, a dynamic en route filtering mechanism that does not exchange explicit control messages for rekeying. Second, provision of one-time keys for each packet transmitted to avoid stale keys. Third, modular and flexible security architecture with a simple technique for ensuring authenticity, integrity and no repudiation of data without enlarging packets with MACs. Forth, A robust secure communication framework that is operational in dire communication situations and over unreliable medium access control layers .The random distribution of data is done by using DES techniques. It is used to provide security in a efficient way. The energy of the sensor is being saved by doing all the encryption and decryption in with the residual energy of the sensor.

IV. MODULES

The virtual energy-based keying process involves the creation of dynamic keys. Contrary to other dynamic keying schemes, it does not exchange extra messages to establish keys. A sensor node computes keys based on its residual virtual energy of the sensor. The key is then fed into the crypto module. The crypto module employs a simple encoding process, which is essentially the process of permutation of the bits in the packet according to the dynamically created permutation code generated via RC4. The encoding is a simple encryption mechanism adopted however, architecture allows for adoption of stronger encryption mechanisms in lieu of encoding.

Last, the forwarding module handles the process of sending or receiving of encoded packets along the path to the sink.

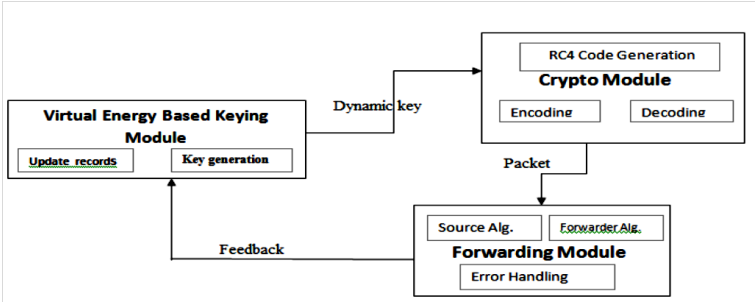

Fig 1. Modular diagram

A. *Virtual Energy-Based Keying module*

The virtual energy-based keying process involves the creation of dynamic keys. Contrary to other dynamic keying schemes, it does not exchange extra messages to establish keys. A sensor node computes keys based on its residual virtual energy of the sensor. Energy-based keying module ensures that each detected packet2 is associated with a new unique key generated based on the transient value of the virtual energy. After the dynamic key is generated, it is passed to the crypto module, where the desired security services are implemented. The process of key generation is initiated when data is sensed; thus, no explicit mechanism is needed to refresh or update keys. Moreover, the dynamic nature of the keys makes it difficult for attackers to intercept enough packets to break the encoding algorithm.

B. *Crypto module*

The crypto module employs a simple encoding process, which is essentially the process of permutation of the bits in the packet according to the dynamically created permutation code generated via RC4. Due to the resource constraints of WSNs, traditional digital signatures or encryption mechanisms requiring expensive cryptography is not viable. The scheme must be simple, yet effective. Thus, in this section, we introduce a simple encoding operation similar to that used in [2].

The encoding operation is essentially the process of permutation of the bits in the packet, according to the dynamically created permutation code via the RC4 encryption mechanism. The key to RC4 is created by the previous module (virtual energy based keying module). The purpose of the crypto module is to provide simple confidentiality of the packet header and payload while ensuring the authenticity and integrity of sensed data without incurring transmission overhead of traditional schemes. However, since the key generation and handling process is done in another module, This flexible architecture allows for

adoption of stronger encryption mechanisms in lieu of encoding. In this module DES technique is used to provide the random packet transmission from source to sink in order to provide security.

C. Forwarding module

The final module is the forwarding module. The forwarding module is responsible for the sending of packets (reports) initiated at the current node (source node) or received packets from other sensors (forwarding nodes) along the path to the sink. The reports traverse the network through forwarding nodes and finally reach the terminating node.

V. ALGORITHMS

In the forwarding module the following algorithms are used to forward packets from source to sink.

A. Source node algorithm

The source node uses the local virtual energy value to construct the next key. The source sensor fetches the current value of the virtual energy from the first module. Then, the key is used as input into the RC4 algorithm inside the crypto module to create a permutation code for encoding the message. When an event is detected by a source node, the next step is for the report to be secured. The source node uses the local virtual energy value and an IV (or previous key value if not the first transmission) to construct the next key. As discussed earlier, this dynamic key generation process is primarily handled by the first module. The source sensor fetches the current value of the virtual energy from the virtual energy based keying module. Then, the key is used as input into the RC4 algorithm inside the crypto module to create a code for encoding the $\langle ID\,|type|data\rangle$ message. The encoded message and the clear text ID of the originating node are transmitted to the next hop (forwarding node or sink) using the following format: $ID,\{ID,type,data\}]pc]$ where $\{x\}pc$ constitutes encoding x with permutation code Pc. The local virtual energy value is updated and stored for use with the transmission of the next report.

B. Forwarder Node Algorithm

Once the forwarding node receives the packet it will first check its watch-list to determine if the packet came from a node it is watching. If the node is not being watched by the current node, the packet is forwarded without modification or authentication. Although this node performed actions on the packet (received and forwarded the packet), its local virtual perceived energy value is not updated. This is done to maintain synchronization with nodes watching it further up the route. If the node is being watched by the current node, the forwarding node checks the associated current virtual energy record (Algorithm 2) stored for the sending node and extracts the energy value to derive the key. It then authenticates the message by decoding the message and comparing the plaintext node ID with the encoded node ID. If the packet is authentic, an updated virtual energy value is stored in the record associated with the sending node.

VI. CONCLUSION

Communication is very costly for wireless sensor networks (WSNs) and for certain WSN applications. Independent of the goal of saving energy, it may be very important to minimize the exchange of messages (e.g., military scenarios). To address these concerns, the presented communication frame work for WSNs is Secure Encryption and keying based on virtual energy. In comparison with other key management schemes, This has the following benefits: 1) it does not exchange control messages for key renewals and is therefore able to save more energy and is less chatty, 2) it uses one key per message so successive packets of the stream use different keys—making more resilient to certain attacks (e.g., replay attacks, brute-force attacks, and masquerade attacks), and 3) it unbundles key generation from security services, providing a flexible modular architecture that allows for an easy adoption of different key-based encryption or hashing schemes. DES algorithm is implemented to increase the security.

Acknowledgement

Our Sincere thanks to the Respected Dean Dr. S. Karthik of CSE Department from SNS Tech, his valuable suggestion and thoughts is motivated to publish this paper and our beloved Head of Department Dr. T. Kalai Kumaran, Computer Science and Engineering from same institution, his excellence and suggestion is very useful towards this paper to publish.

References

1. A.S.Uluagac, R.A.Beyah, Y.Li, "VEBEK: Virtual Energy-Based Encryption and Keying for Wireless Sensor Networks" IEEE Trans. Mobile Computing, vol.9 no 7, July 2010.
2. H. Hou, C. Corbett, Y. Li, and R. Beyah, "Dynamic Energy-Based Encoding and Filtering in Sensor Networks," Proc. IEEE Military Comm. Conf. (MILCOM '07), Oct. 2007.
3. M. Ma, "Resilience of Sink Filtering Scheme in Wireless Sensor Networks," Computer Comm., vol. 30, no. 1, pp. 55-65, 2006.
4. V. Rahunathan, C. Schurgers, S. Park and Mani B. Srivastava, "Energy Aware Wireless Sensor Networks", pp.1-17; Dept of Elec Eng, Uni of California, L. A, 2004.
5. S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An Interleaved Hop-by- Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks," Proc. IEEE Symp. Security and Privacy, 2004
6. A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. Tygar, "Spins: Security Protocols for Sensor Networks," Proc. ACM MobiCom, 2001.
7. M. Luk, G. Mezzour, A. Perrig, and V. Gligor, "Minisec: A Secure Sensor Network Communication Architecture," Proc. Sixth Int'l Symp. Information Processing in Sensor Networks (IPSN '07), pp. 479-488, Apr. 2007
8. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci,"Wireless Sensor Networks: A Survey," Computer Networks,vol. 38, no. 4, pp. 393-422, Mar. 2002.
9. C. Vu, R. Beyah, and Y. Li, "A Composite Event Detection in Wireless Sensor Networks," Proc. IEEE Int'l Performance, Computing, and Comm. Conf. (IPCCC '07), Apr. 2007.

AUTHOR(S) PROFILE

S.P.Santhosh Kumar, is presently working as a Assistant Professor in SNS College of Technology, Coimbatore, India and he is having four years of Industrial Experience. His research interest focuses on Wireless Networks, Internet Programming and Software Engineering

C.B.Sivaparthipan, is now working as an Assistant Professor at SNS College of Technology, Coimbatore – India and his area of interest mainly focusing on Mobile Ad-Hoc Network with Data Mining Application.

Prabakar.D, At present, He is an Assistant Professor of Computer Science and Engineering in SNS College of Technology, Coimbatore. His research interest focuses on Wireless Communication, Mobile Computing and Wireless Sensor Networks.

Dr.S.Karthik, is presently Professor & Dean, Department of Computer Science & Engineering, SNS College of Technology, affiliated to Anna University- Chennai, Tamilnadu, India. M.E Degree and Ph.D Degree from Anna University Chennai.His research interests include network security, web services and wireless systems. Dr.S.Karthik published many papers in international journal and conference papers and has been involved many international conferences as Technical Chair and tutorial presenter. He is a active member of IEEE, ISTE and Indian Computer Society.

