Middle-East Journal of Scientific Research 25 (3): 603-615, 2017
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2017.603.615

Taxonomy of Attacks and Secure Data Aggregation Mechanisms for Smart Environment

Amirthavalli Madhwaraj and Chithra Selvaraj

Research Center, Department of Information Technology,
SSN College of Engineering, Chennai, India

Abstract: Internet of Things (IoT) is a paradigm of pervasive presence in the environment of disparate smart components. An efficient and secure data aggregation technique plays a major role in aggregating data from low powered smart devices in a secure way. Additionally, the aggregation technique should adhere to security principles to ensure the reliability of data. The limitations and geographical jurisdiction of smart devices make themselves vulnerable and prone to diverse forms of threats. In this article, a survey has been carried out on data aggregation related attacks for smart networks. The security goals and various security mechanisms on data aggregation have been studied in detail. Further, the comparative study of various secured data aggregation mechanisms has been performed based on security goals. The open challenges and the directions for research have been discussed. This survey would serve as a complete review of attacks and secure data aggregation in IoT.

Key words: Internet of things · Data aggregation · Security · Attacks

INTRODUCTION

Internet of Things (IoT) is a paradigm of pervasive presence in the environment of disparate smart components. An IoT device consists of sensors, actuators, communication interface, operating systems, system software, preloaded applications and lightweight services. These objects are decomposed into different layers of abstraction for standardization and reliability. The things layer containing smart devices and actuators to generate data that is specific to the type of device used. Aggregation Layer is entrusted with the task of collecting raw data from several IoT devices and calculates a small message that summarizes the important information for transmission [1]. Two levels of aggregation are performed resulting in in-network or multiple aggregations. Otherwise, single level of aggregation is performed [2]. The network layer addresses routing schemes and unique identification scheme connects the smart objects through wired and wireless infrastructure. The primary functionality of database management layer is to support the storage of big data generated by abundant IoT networks in an authorized, authenticated storage environment. Data produced by the node can be stored either in a local storage infrastructure and the cloud infrastructure. These are enriched with storage space and functionalities to store streaming and non-streaming data to provide global aggregate of assorted data [3, 4, 5]. The application layer focuses on novel approach of programming model should be devised for creation of autonomous, context-aware and service-oriented objects adding elegance to IoT architecture. Security component is added to each of the layer to protect data, device and network from endanger.

The deployment and positioning of IoT objects may also exhibit security issues that hinder aggregation process and services offered by its counterparts. As a result, diverse attacks to breach security goals can be launched by an adversary to obtain sensitive data Secure data aggregation refers to the efficient delivery of summaries of measured data from the sensor network to an off-site user in such a way that the user can have high confidence that the reported data summaries have not been manipulated by an adversary [6]. The security mechanisms adopted in WSN data aggregation scheme can be an excellent candidate for integrating in IoT data aggregation environment.

Corresponding Author: Amirthavalli Madhwaraj, Research Center, Department of Information Technology,
SSN College of Engineering, Chennai, India.

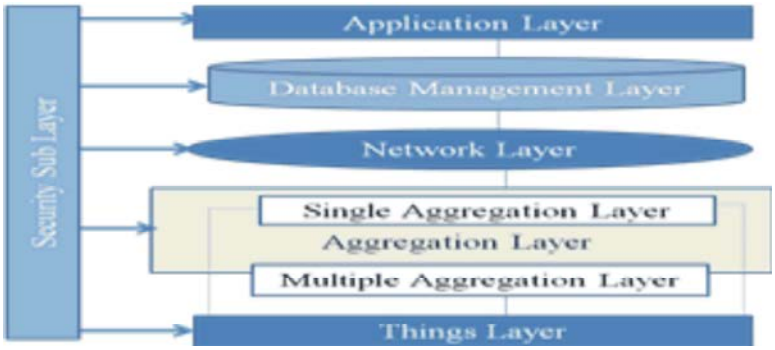

Fig. 1: Data Aggregation Oriented IoT Architecture

The outline of this article is to emphasize on the types of attacks that are evident in aggregators and security issues. Also, to study the security requirements and security protocols in the context of data aggregation in WSNs since no substantial work has been done for IoT systems in general have been enumerated in the survey.

Concepts of Data Aggregation: Data aggregation is an ideal conceptual design to overcome the resource constraints of IoT objects in terms of energy and computational power.Data aggregation is the process of collection of data(d_1, d_2, …., d_n) from multitude smart devices (sd_1, sd_2…, sd_n) and summarizing individual data into a single comprehensive aggregate digest (AD) by a special purpose smart devices called aggregators [6]. An aggregate digest (AD) is denoted by equation (1).

$$AD = \sum_{i=1}^{n} sd_i \quad (1)$$

The core principles of aggregation are explained in Figure 2. An aggregator is augmented with aggregate function to perform aggregation. The most commonly used aggregate functions are listed in Table 1. The aggregated data is transmitted to an intermediate sink node, also known as base station (BS). A base station can unicast or multicast data to final sink nodes(s). The final sink can be a user, another IoT device, mobile gadget or a server.

Network Environment: The primary elements at the lowest level of IoT architecture of Figure 1 can be arranged in a particular fashion to reduce energy consumption and communication latency. The elements required in a network environment are described as follows. Each node can form downstream or upstream nodes in forwarding messages between source and destination.

Leaf nodes are IoT devices with smart intelligence and participatory sensing. These nodes are designed with real-time functionality and are deployed in hostile environment. They produce sensing data that can be used to monitor a real-time situation.

Aggregation node or aggregator can be assumed to be an object with high memory capacity and energy level compared to leaf node which assimilates and fuses data generated by leaf nodes. Some sensor nodes are designated as data aggregators to aggregate data from their neighboring sensor nodes besides sensing raw data.

Sink node can be a single aggregator / base station (BS) or gateway that receives the final encrypted aggregate value from the whole network, decrypts it and forwards the data to diverse forms of recipient as shown in Figure 2.

Aggregation Topologies: The aggregation process purely depends on the organization of nodes. Based on the literature survey, three types of topology are identified [7, 8, 9]. In Chain based aggregation each IoT device transmits only to its closest neighbor in a homogeneous network [7]. Basically, the topology resembles a chain connecting a leaf node and sink with hop count between them may vary as evident in Figure 3(a). A hierarchical organization of the nodes forms a tree structure in a network. As an initial step of tree construction, a spanning tree would be created having the sink node as the root. Subsequently, the sink discovers IoT nodes and aggregation nodes within the communication range by exchanging query messages resulting in tree formation is shown in Figure 3(b). The advantage of tree-based approach is reduced end-to-end delay [9]. This topology is known as tree based aggregation. Any number of arbitrary nodes can form a cluster either manually or automatically. A cluster head would be nominated internally in a cluster of nodes based

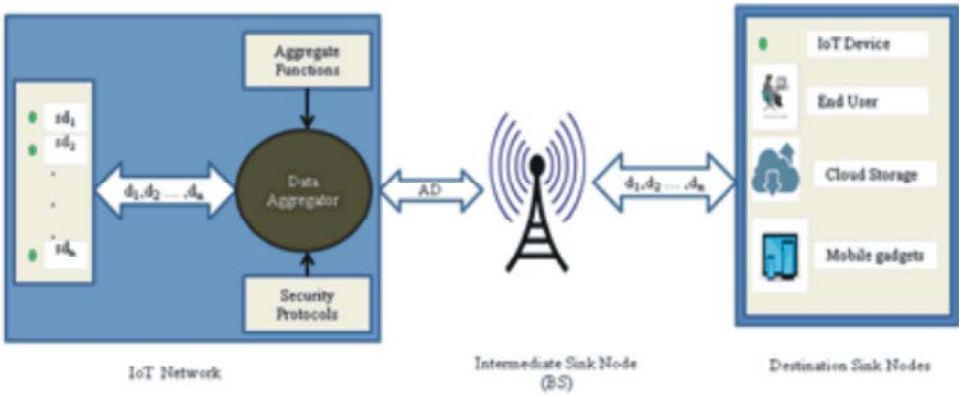

Fig. 2: Generic Principles of Data Aggregation in IoT

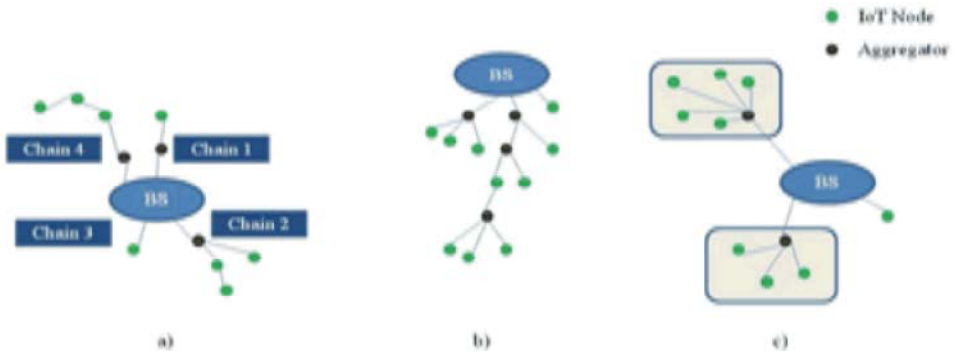

Fig. 3: Topology of Data Aggregation Nodes a) Chain topology b) Tree topology c) Cluster topology

on various parameters like its residual energy and the node's proximity to its neighbors. This approach is known as cluster based aggregation and depicted in Figure 3(c) [11]. The advantage of this approach is reduction in energy dissipation and scalability [12].

Adversary Model: The intention of an adversary is to violate the security goals of an aggregation system. Adversary classification can be made on the basis of corruption strategy, adverse behavior and complexity.

Corruption Strategy: The strategy explores possible options to violate security requirements and encroachment of various nodes in IoT network. Two types of strategy are adopted to perpetrate an attack. First, in static corruption mode, the honest nodes in the aforementioned topology remain honest and adulterated node remains corrupted. Secondly, in the adaptive corruption mode chooses a set of nodes on fly. It can be discussed under two scenarios. The first case, involves an adversary choosing a set of aggregator nodes, so as to deviate the values of the aggregation digest. In the second scenario, happens when any arbitrary number of leaf nodes is compromised to report false data as the computation of aggregation process is in progress [13].

Adversarial Behavior: The suspicious nature of activities carried out by an adversary can be classified into three types. In a semi-honest adversary model follow data aggregation protocol specification that creates passive adversarial effect. An adversary can launch an active attack to corrupt honest nodes is termed as malicious adversarial model. A covert adversary arbitrarily affects honest nodes in clandestine manner [13].

Computation Complexity: The computation complexity of the adversary depends on the execution time of a mechanism. Timing attacks can be perpetrated by an adversary. Based on this, two adversarial classifications can be made. Firstly, an adversary executes an aggregation protocol in polynomial time. Secondly, an adversary can use unbounded computational power [13].

Taxonomy of Security Attacks: Attacks are launched to disrupt the normal operation either to cause destructive effect or for surveillance. In IoT environment, due to its openness, device specific features and vulnerabilities in planting intelligent autonomous products either in Internet connected or partially connected architecture may lead to various security attacks. The attacker could be an outsider (unauthorized) node that does not possess

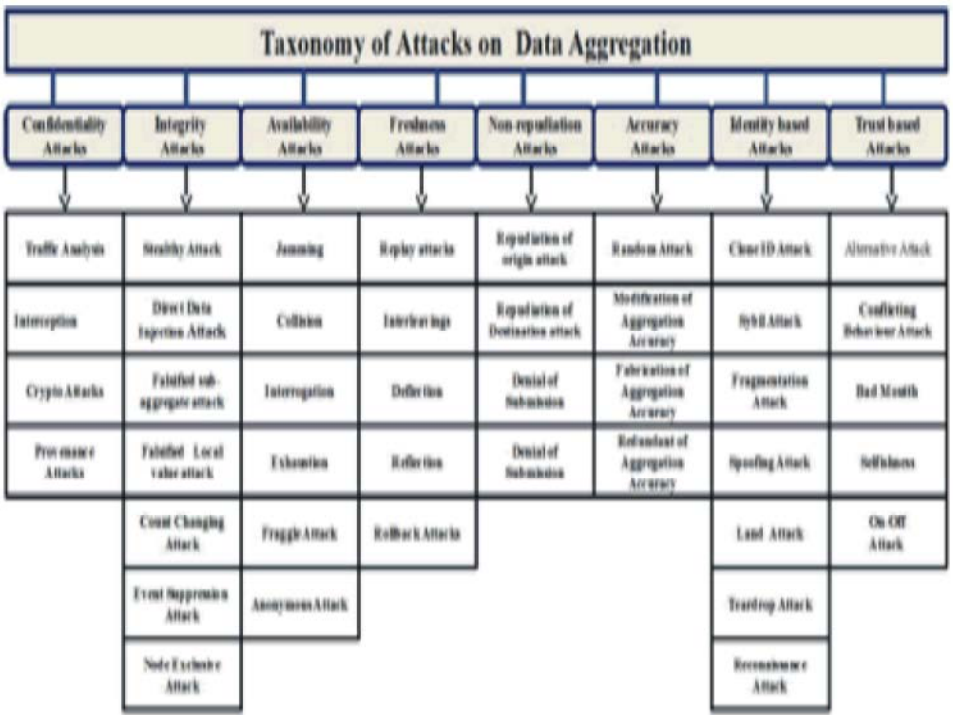

Fig. 4: Attack Taxonomy

a valid credential, an insider (authorized) or a compromised node that possesses a valid credential [14]. The activities of the compromised node can create a major impact on the resultant aggregated value. The risks posed to aggregated data are numerous and derive from both external and internal threats [15]. A vulnerable node can be compromised to launch passive or active attack based on the intention of an adversary. The conventional attacks as enumerated in the following sub sections can cause a serious threat to manipulate the values transmitted by set of IoT devices and the data handled by data aggregation process. The anatomy of attacks is tabulated from Table 2 to Table 9. These typical attacks as visualized in Figure 4 can be envisaged in IoT environment.

Confidentiality Attacks: The original sensed data and the intermediate aggregation results are disclosed to the unauthorized parties during the transmission of information. The privacy of IoT object and their correspondence between various nodes in the topology would be under threat. As a consequence, an end to end confidentiality of the information to be transmitted is affected. The categorization of confidentiality attacks is shown in Table 2.

Integrity Attacks: The consistency of raw data and aggregated data can be adjusted to inject false data into the network during both transmission and aggregation process. A compromised node can also directly change value to forge the base station. Individual IoT nodes or an aggregator can lie about the measurements, digests and aggregated reports. All these attacks are collectively referred to as content attacks [19]. End-to-end integrity prevents the attacks that target the integrity of packets [20]. The categorization of integrity attacks that are possible are listed as shown in Table 2. Integrity attacks can be countered by robust watermarking techniques, keyless Signature Infrastructure (KSI) is designed to provide scalable digital signature based authentication using hash-function cryptography [21].

Availability Attacks: The notion of this attack is to impede the availability of system resources and service delivery. There must be a guaranteed aggregation service by an aggregator. An adversary node is a node in IoT architecture that can deny system and network resources and application specific services. The popular availability attack is denial of service (DoS). DoS attacks are classified as no-data attacks and garbage data attacks. In no-data DoS attack, the resource is depleted by exchange of short

Table 1: Confidentiality attacks

Type	Description	Impact
Crypto Attack	Breach of secure data aggregation algorithms in order to reveal or manipulate sensitive information [16].	Circumventing security of protocol, key management scheme and cipher text
Traffic Analysis	Analysis of communication pattern between sensor node, aggregation node and base station [17].	Tracking the location of three nodes to cause jamming effect or denial of service [16].
Interception	Data interception between IoT node, aggregator node and sink	Unauthorized access to confidential information
Provenance Attack	The legacy of information exchanged between various nodes in network is exposed	Disclosure of itinerary information [18].

Table 2: Integrity attacks

Type	Description	Impact
Stealthy attack	False aggregation results that are significantly different from the original results are transmitted to the base station [20].	Mislead the requestor from getting any aggregation result [22].
Direct Data Injection	A malicious aggregator modifies the data reported by its directly controlled leaf node [5].	Modification of aggregated values [5, 23].
False Data Injection	A base station may receive false aggregation reports from aggregator nodes [24].	End-to-end integrityis violated.
Falsified sub-Aggregate	Falsifies the aggregation result preventing from or misleading the requestor from accessing the value [24].	Lack of accuracy.
Falsified Local Value	Any IoT device can intentionally falsify its own value. This attack happens due to faulty device or false data injection attack [24].	The identity of nodes associated in network is hidden.
Count Changing	Count value indicating the number of sensor nodes involved in the aggregation operation is modified [26].	Integrity of a sink node is affected
Inflation	The compromised node can inject a large amount of error in the final estimate of the sink node [25].	Lack of accuracy.
Deflation	The aggregate estimate of sink is being lower than the original estimate [25].	The attack might cause threat to real-time critical systems,
Event Suppression	The compromised node changes its aggregated value corresponding to real abnormal events to a normal value [25].	Lack of accuracy
Node Exclusive	A malicious node can intentionally exclude the value of a single or specific group of nodes. [25]	Lack of accuracy

Table 3: Availability attacks

Type	Description	Impact	
Jamming	A jammer would be implemented with legitimate wireless communications	Preventing the transmission and reception of packets between source and sink node [28].	LDoS
Collision	Target the MAC layer of any node in IoT network to cause exponential back off.	More energy expended to cause depletion of energy.	LDoS
Interrogation	Repeatedly sending messages to elicit responses from a targeted node [29].	Computation overhead and exhaustion of resources	LDoS
Exhaustion	Retransmitting a message to recipient nodes due to collision.	Maximum link utilization by a source node causing energy exhaustion of a recipient	LDoS
Fraggle attack	Sending a large amount of spoofed TCP/UDP traffic to broadcast address within network by an aggregator node [30]	Resource depletion of victim. node.	FDoS
Anonymous Attack	An unidentified remote node can launch DoS attack to disrupt aggregation process	▪ Increase in aggregation latency.	FDoS or LdoS

Table 4: Freshness attacks

Type	Description	Impact
Replay attack	An unauthorized node captures network traffic and retransmits data over period of time.	Interruption of traffic and subverting data security to violate integrity goal.
Interleaving	The sequence of sensed data values and aggregated messages may be interleaved [32].	Consistency and serialization of aggregation process are violated
Reflection	The sensed data values or aggregated messages are directed towards the source [32].	Base station need not be contemporaneous
Deflection	Old or new messages are being diverted to a third party [32].	Fabrication of messages
Rollback	A compromised node can restore its previous data [31].	Integrity and consistency violations.

Table 5: Non-Repudiation Attacks

Type	Description	Impact
Repudiation of Origin	A dishonest originator node does not guarantee that it has sent data to recipient [33].	▪ Frequent retransmission of messages. ▪ Denial of service by originator.
Repudiation of receipt.	A dishonest node does not acknowledge the data received from the originator [34].	Dropping of messages causing inconsistency.
Denial of submission	A dishonest originator node disagrees to trusted third party (TTP) that it has submitted the aggregation information to recipient [34].	Denial of service by originator.
Denial of Delivery	A dishonest recipient node disagrees to trusted third party (TTP) that it has received the aggregation information from the originator [34].	Diversification of message to illegitimate node.

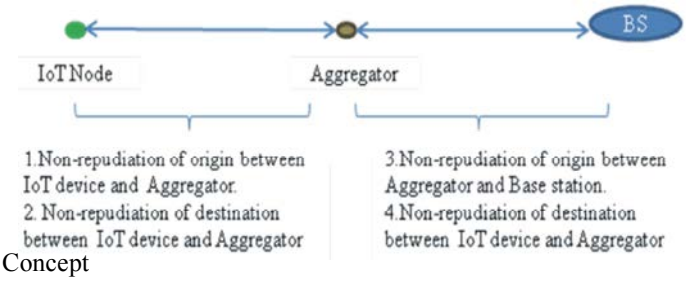

Fig. 5: Non-repudiation Concept

Table 6: Accuracy Attacks

Type	Description	Impact
Random attack	A dishonest node in the network can inject some arbitrary values to aggregation result.	Integrity of message is affected.
Modification	The aggregation result can be modified by a malicious node.	Integrity of message is affected.
Fabrication	The attack inserts a new value to aggregation result.	Integrity of message is affected.
Redundancy [35]	Duplicate values can be inserted to aggregation result intentionally by malicious node.	Integrity of message is affected.

Table 7: Identity Attacks

Type	Description	Impact
Clone ID Attack	Replication of vulnerable node by an adversary to launch variety of malicious activities [37].	Biasing aggregation result.
Sybil Attack	Creation of multiple logical identities on the same physical node by a Sybil node [38].	Network performance degradation.
Spoofing Attack	An attacker can forge its identity to masquerade as another device or even create multiple illegitimate identities in network.	Modification of aggregation results
Fragment Duplication	An attacker launching a fragmentation type of attack can proactively block processing of any fragmented packet at the target node by sending a single fragment [39].	Modification of aggregation results
Buffer Reservation Attack	Duplication of an overheard fragment of the sender and transmits it to the recipient	Disambiguate in fragments [39].
Reconnaissance Attack	An intruder uses active scanning methods to identify addresses and ports of victim network to execute a nefarious act [40].	Selective forwarding of messages to sink node
Land Attack	The source and recipient IP address are same. This attack can be executed at any node in the topology [41],	Indefinite loop is caused

Table 9: Trust Based Attacks

Type	Description	Impact
Alternative attack [43]	A compromised node switch to other kind of misbehaviours due to the fluctuation in reputation value.	Distort data aggregation result.
Conflicting behaviour [44]	Different behaviour for different set of nodes in the topology.	Concocted values are generated by each node
Bad-mouth [42]	An attacker node spread false information about trustworthy node to decrease the trust rating.	Integrity and consistency affected
Selfishness [45, 46]	An attacker node spread false information about trustworthy node	Decrease in trust rating
On-off attack [47]	A malicious node alternatively switches the behaviour between trusty and untrustworthy node to keep trust level above threshold.	Deviation in aggregation result
Selective Behaviour attack [48]	A partial behaviour of accepting recommendations from a subset of nodes.	Deviation in aggregation result.

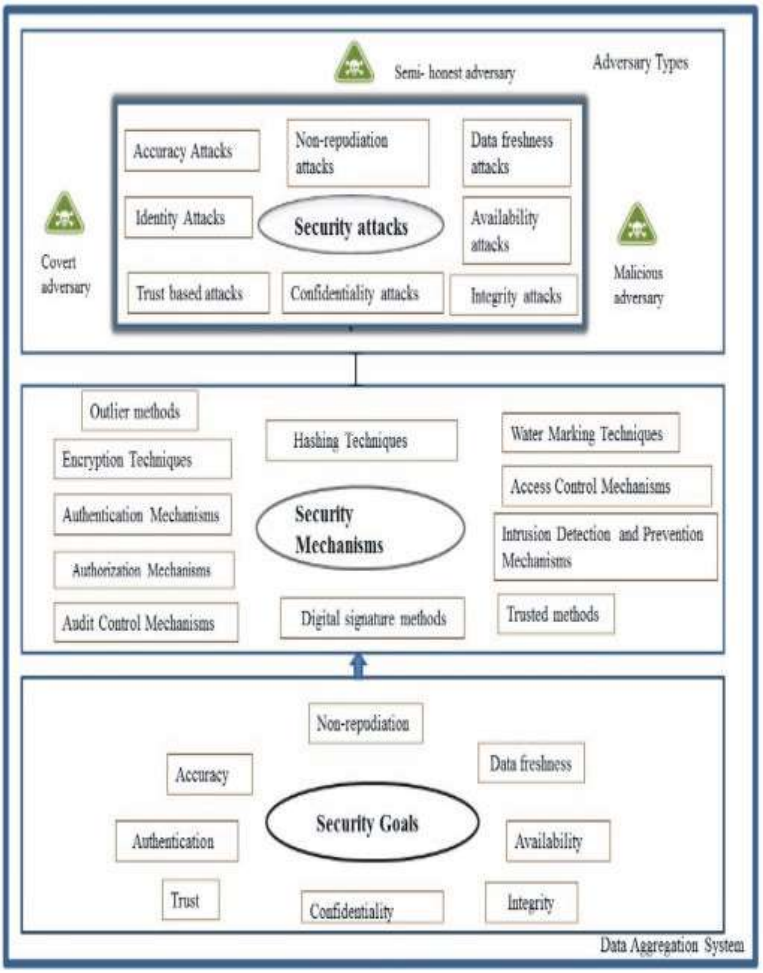

Fig. 6: Secure Data Aggregation Architecture

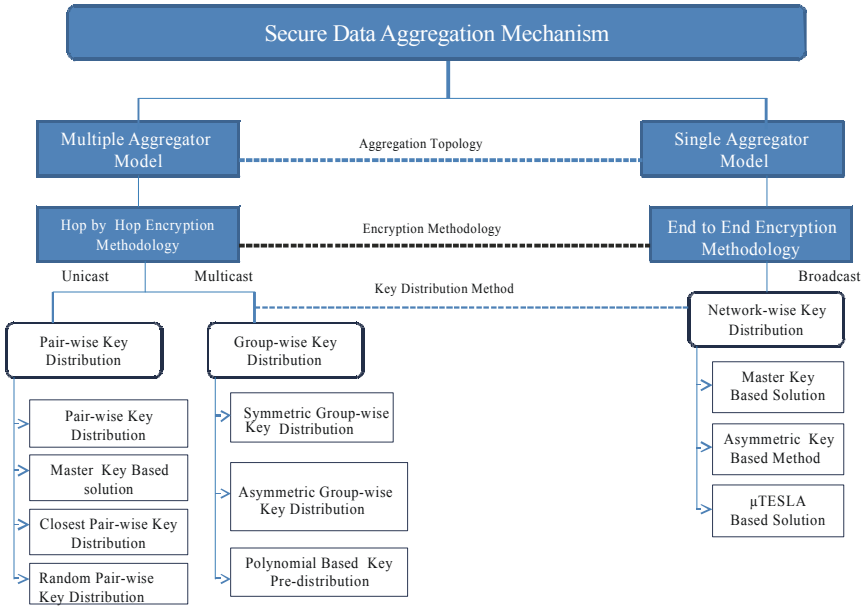

Fig. 7: Hierarchical Classification of Secure Data Aggregation

Table 10: Relationship between Security Services and Security Mechanisms

Security Services	Security Mechanisms
Confidentiality	Symmetric and asymmetric encryption, homomorphic encryption, traffic padding mechanisms
Integrity	Hash and Message authentication code(MAC) functions, digital signature schemes, watermarking techniques, notarization techniques.
Availability	Access control mechanisms, confidentiality mechanisms.
Freshness	Integrity mechanism with nonce and timestamp.
Accuracy	Integrity mechanisms and outlier techniques
Identity management	Public key authentication mechanism, zero-knowledge proofs, digital signatures, one -time passwords.
Non-repudiation	Digital signature with certificate, digital signature with TTP.
Trust	Ratings, weighting, probability, neural network, Bayesian network, fuzzy logic, swarm intelligence, directed and undirected graph.

bursts of data minimizing the data rate. It is also referred as Low-rate DoS (LDoS) attacks due to congestion caused by adversary. The goal of garbage data DoS attack is to flood a victim's node with garbage data. This is also known as flood DoS(FDoS) [27]. The taxonomy of DoS attacks is shown in Table 3.

Data Freshness Attack: Freshness is an important security attribute that can be exploited to create an adverse effect to disrupt normal sequence of operations. An adversary can mislead the recipients by sending the expired data to them. Freshness attack can be explored at two levels. At the first level, any leaf node can send old data to aggregator. The second level includes sending of aggregated values that too are old to the base station. The details of different types of possible freshness attacks are tabulated in Table 4.

Non-Repudiation Attacks: The non-repudiation property in data aggregation ensures that any node in the network cannot deny their participation in aggregation process. The first pair of non-repudiation of origin emphasize that leaf node assure that it has forwarded the sensed data to aggregator. Further aggregation node does not deny that aggregated value has been sent to sink node. Likewise, the non-repudiation of destination also happens among these three nodes. The goal of non-repudiation can be violated by launching various attacks as listed in Table 5. Generally, these attacks are termed as repudiation attacks.

Accuracy Attack: Data aggregation results may be used to make critical decisions in the event driven application. Any outlier value can the accuracy of final aggregation result at root node is very important for any data aggregation scheme [35]. The final decision at the sink node is based on the aggregation accuracy. However, the accuracy of aggregation result can be forged to yield an inaccurate value by executing the attacks as shown in Table 6.

Identity Attacks: The vital component in IoT protocol stack is identity /addressing facilitates in recognizing the objects. The IoT will include a very large number of nodes, each of which will produce content that should be retrievable by any authorized node. Identifiers play a critical role for retrieval of information from repositories and for lookup in global directory lookup services and discovery services, to discover the availability and find addresses of distributed resources [1]. The embedded devices instilled in IoT entities depend on shared wireless media for data transmission that is vulnerable to perpetrate an attack. A malicious node can gather identity information to launch identity based attacks [36]. The various types of attacks are listed in Table 8.

Trust Based Attacks: Trust is the degree of belief about the future behaviour of other entities, which is based on the one past experience and observation of the others actions [42]. Trust management can help improving the security of data aggregation of IoT to provide light-weight trust based approaches that are very useful to deal with node misbehavior to enhance security features. The trust-based attack taxonomy is shown in Table 9.

Security Architecture for Data Aggregation System: Prior to developing a defense strategy, the following three concepts must be assessed by a security expert based on the X.800 security architecture for OSI that can be imbibed for data aggregation system. The construction of secure data aggregation architecture is shown in Figure 6.

Security Services: The conventional security design goals are applicable in IoT scenario as illustrated in Figure 6 resembles Parkerian Hexad model [49]. Security services are goals adhered by security mechanisms to build a robust defense method methodologies to thwart various types of attacks. Secure data aggregation encompasses the following security requirements:

Data Confidentiality is the ability to protect the aggregated data of various IoT devices from disclosure to unauthorized parties.

Integrity refers to the ability to prevent an aggregated data from being changed in an unauthorized or undesirable manner.

Availability refers to aggregators that are obliging to perform aggregation on authorized IoT devices.

Non-repudiation service ensures that aggregator and IoT device do not deny the origin and delivery of data transmitted between them for data processing.

Authentication is a process by which a system verifies the identity of an IoT device as the transmitter of data, known as message authentication and aggregator as the receiver of data, referred to as entity authentication.

Accuracy refers to the extent by which the aggregated value matches with the value generated by individual IoT nodes [50]. Raw data accuracy in leaf node and aggregation data accuracy are critical parameters to estimate the accuracy of base station.

Freshness ensures that the data are recent and that no old messages have been replayed to protect data aggregation schemes against replay attacks. It also emphasizes that aggregation output from an aggregator must be current based on the current information created by a group of IoT devices.

Trust refers to the reliability of an aggregator with strong sense of security without compromising for denial of service or misinterpretation of data.

Security Mechanisms: Security mechanisms are computationally designed methods to enforce security goals. The objective of any security mechanism is to detect, protect and prevent from any security vulnerability. There are various standard security mechanisms are available for wired and wireless networks. A comparative study of various security protocols that addresses diverse security goals, type of encryption method based on the literature survey has been listed in Table 14.

Data aggregation schemes must entail security mechanisms to instill aforementioned security goals to protect data and the device in entirety. Data aggregation security can support multiple interdependent security domains such as physical security, network security and data security safeguarding the device and data from unauthorized disclosure and modification [51, 57]. The hierarchical classification of secure data aggregation mechanisms is shown in Figure 7. The first level of hierarchy represents the security type done on the basis of aggregation topology. The second level of hierarchy focuses on the security mechanisms for data aggregation that can provide either one of the following services based on encryption methodology adopted by the network. The third level of hierarchy is based on key distribution techniques which is dealt in the next section. The relationship between security services and conventional security mechanisms are shown in Table 10. The conventional security mechanism has to be adjusted to meet the requirements of small sized IoT nodes.

Encryption Methodology: Encryption methodology adopted by the aggregation layer uses homomorphic encryption. A homomorphic cryptosystem is a cryptosystem with an efficient algorithm to compute an encryption of the sum or the product, of two messages given the public key and the encryptions of the messages but not the messages themselves. The different types of encryption method are as follows:

Hop-by-Hop Encryption Method: The sensed data encrypted by leaf node is decrypted by aggregation node to perform aggregation during its course of travel from leaf node to sink node. This method is susceptible to confidential attacks. Besides, cost incurred by an aggregation node to decrypt data of each leaf node is high. Therefore, this method is not widely used in sensitive application [52].

End-to-End Encryption Method: The sensed data encrypted by leaf node cannot be decrypted by aggregation node. It aggregation node applies aggregate function on encrypted data. This method ensures confidentiality and data privacy [52].

Fig. 8: Hop-by-Hop Encryption Scheme

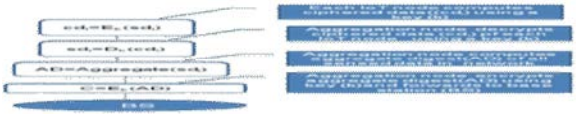

Fig. 9: End-to-End Encryption Scheme

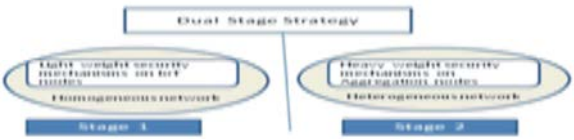

Fig. 10: Dual Stage Security Scheme

Dual Stage Strategy: Each network stage applies different security approaches depending on the resource capacity. Nodes with limited resource are grouped as homogeneous network applying lightweight security algorithm. In contrast, nodes with high resource are grouped as heterogeneous network built with robust and complex security algorithms [52].

Related Work: The security mechanisms adopted in WSN data aggregation scheme can be an excellent candidate for integrating in IoT data aggregation environment The comparison of various security mechanism available for data aggregation collected from the literature survey is tabulated in Table 14.The comparison is done based on the security goals , type of encryption methodology and the attack resilient. The implications of adopting these security techniques in IoT can be considered for analysis in terms of energy, memory and processing overhead.

Security Challenges: Data aggregation is a paramount process at the device level to overcome the inherent qualities of smart objects that can pose a serious threat to security. The essential vulnerable issues of any data aggregation schemes listed below can be research directions that can be considered for designing a robust IoT aggregation systems.

General Issues: Security classification, information classification based on confidentiality and integrity models, geographic jurisdiction of nodes, service level agreement of neighbouring nodes and base station can be a generic security draft.

Spatial and Temporal Issues: The spatial parameters are code size, data size and location attributes of smart objects. The temporal parameters are computation time and battery lifetime of an object. The probability of launching attacks on a remotely deployed object based on these parameters are high. The quality of these parameters can be analyzed to draft a security classification.

Physical Challenges: The protection and control of smart objects, change in device properties and configureuration can pose a serious threat to users of service. A mechanism to combat this challenge is a major concern of research issue. Machine learning and behavior analysis can be employed in determining safe device behavior and general usage patterns.

Logical Challenges: This includes authorization and authentication mechanisms to establish identity to exercise rights over accessing the nodes. Access control mechanism and secure third party arbitration like Kerberos system can facilitate safe usage of nodes and data.

Network Challenges: The protection of wireless communication infrastructure to combat eavesdropping in the channel connecting leaf node, aggregator node and base station using light weight encryption methods that can be added as a field to the existing routing protocols such as 6LoWPAN, RPL and any adhoc and wireless network protocols. The performance analysis in terms of computation complexity, communication overhead, security and battery usage can be calculated for efficiency and robustness.

Data Security: Spurious data points can be inserted as an outlier either by an event or by a malicious attack. Machine learning and ensemble and hybrid methods can be employed in to spot and remove outlie to improve accuracy. Also, to detect and block anomalous behavior of tampering data and intrusion.

Cryptographic Challenges: Optimized asymmetric encryption methods such as, Tiny ECC, Zero-knowledge proofs (ZKP), NTRUEncrypt, fusion of symmetric and asymmetric algorithms can be applied to study the security and performance analysis of three nodes involved in aggregation process.

CONCLUSION

Internet of things encompasses plethora of intricate logical and physical components that are interwoven with one another to bring a new dimension in the field of data communication and network. Secure data aggregation scheme is an important mechanism to combat various security threats, attacks and also to enforce security on data aggregation scheme. A detailed survey of possible data aggregation attacks based on the violation of security goals can be envisaged for IoT environment. Further, key distribution mechanism is also explored as part of the survey. The literature survey on recent security mechanisms for data aggregation have given new insights where security goals like non-repudiation, trust and freshness are least analyzed. Infusion of machine learning concepts to enhance security of the data aggregation nodes can be a future research work.

Mechanism	C	I	A	F	NR	Ac	IM	T	E2E security	HbH security	Attack Resilient
SPKC[28]	★	★				★			★		Stealthy
APHA[65]	★	★		★		★	★		★		
CLWDA [66]						★	★		★		
E-SHM [67]		★				★			★	★	Malleability
SAMOS [68]			★				★		★	★	DoS
SDAW [69]	★	★				★			★	★	
DyDAP [70]		★				★	★		★		
MAI[71]		★				★	★			★	False data injection
Roy *et al* algorithm [72]		★				★				★	Falsified sub-aggregate
CDAMA [73]	★		★							★	Direct Data injection
ETMAM [74]								★	★		
Yun Liu *et al* algorithm[75]						★		★	★		
Sen-SDA [76]		★					★		★	★	
SRDA[51]		★				★		★		★	Alternative attacks

REFERENCES

1. Hu, L. and D. Evans, 2003. Secure Aggregation for Wireless Networks, (2003), Proceedings of Symposium on Applications and the Internet Workshops, pp: 384-390.
2. Fasolo, E. and M. Rossi, 2007. DEI, In-network Aggregation Techniques for Wireless Sensor Networks: A Survey, (2007), IEEE Wireless Communications, 14: 70-87.
3. Vermesan, O., P. Friess, P. Guillemin, S. Gusmeroli, *et al*., 2011. Internet of Things Strategic Research Agenda, Chapter 2 in Internet of Things - Global Technological and Societal Trends, River Publishers.
4. Cooper, J. and A. James, 2009. Challenges for Database Management in the Internet of things. IETE Technical Review, (2009), 26(5): 320.
5. Chan, H., A. Perrig, B. Przydatek and D. Xiaodong, 2007. Song.SIA: Secure information aggregation in sensor networks., (2007), Journal of Computer Security, 15: 69-102.
6. Gelareh Taban, 2008. Dissertation: Secure and Private Data Aggregation in Wireless Sensor Networks", 2008, University of Maryland.
7. Lindsey, S., C. Raghavendra and K.M. Sivalingam, 2002. Data gathering algorithms in sensor networks using energy metrics, (2002), IEEE Transaction on Parallel and Distributed Systems, 13: 924-935.
8. Przydatek, B., D. Song and A. Perrig, 2003. Secure information aggregation in sensor networks, ACM Conference on Embedded Networked Sensor Systems.
9. Cam, H., S. Ozdemir, P. Nair and D. Muthuavinashiappan, 2003. ESPDA: Energy-Efficient and secure pattern based data aggregation for wireless sensor networks, Proceedings of IEEE Sensors, pp:: 732-736.
10. Lee, M. and V.W.S. Wong, 2005. An Energy-Aware Spanning Tree Algorithm for Data Aggregation in Wireless Sensor Networks, (2005), Published in: IEEE Pacific Rim Conference on Communications, Computers and signal Processing, pp: 300-303.
11. Younis, O. and S. Fahmy, 2004. HEED: a Hybrid Energy-efficient Distributed Clustering Approach for Adhoc Sensor Networks, IEEE Trans. On Mobile Computing, pp: 366-379.
12. Sajedi, H. and Z. Saadati, 2014. A Hybrid Structure for Data Aggregation in Wireless Sensor Network, Journal of Computational Engineering, pp: 1-7.
13. Hazay, C. and Y. Lindell, 2010. A Note on the Relation between the Definitions of Security for Semi-Honest and Malicious Adversaries, IACR Cryptology ePrint Archive.
14. S.Zhu, S., S. Xu, S. Setia and S. Jajodia, 2006. LHAP: A lightweight network access control protocol for ad hoc networks, Ad Hoc Networks, 4: 567-585.
15. Michael J. Cerullo, 2005. Threat Assessment and Security Measures Justification for Advanced IT Networks, Information Systems Control J., 1: 35-43.
16. Mitrokotsa, Melanie, Tanenbaum, 2010. Classifying RFID attacks and defenses, Information System Front, pp: 491-505.
17. Zia, T., 2006. Security Issues in Wireless Sensor Networks", International Conference on Systems and Networks Communications (ICSNC).
18. Deng, J., R. Hab and S. Mishra, 2004. Intrusion Tolerance and Anti-Traffic Analysis Strategies for Wireless Sensor Networks, Proceedings of the International Conference on Dependable Systems and Networks, pp: 637-646.
19. Shahriar Bijani and David Robertson, 2014. A review of attacks and security Approaches in open multi-agent systems, Artificial Intelligence Review, pp: 607-636.

20. O.Rafik, O. and M. Boudia, 2015. A novel secure aggregation scheme for wireless sensor networks using stateful public key cryptography, Ad Hoc Networks, 32: 98-113.
21. https://guardtime.com/ksi-technology.
22. Yu, Y., 2012. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures, Journal of Network and Computer Applications, 35: 867-880.
23. Miyaji, A. and K. Omote, 2010. Efficient and Optimally Secure In-Network Aggregation in Wireless Sensor Networks, Chapter Information Security Applications, 6513: 135-149.
24. Roy, S. and M. Conti, 2009. Secure median computation in wireless sensor networks, Ad Hoc Networks, 7: 1448–1462.
25. Roy, S., M. Conti, S. Setia and S. Jajodia, 2012. Secure Data Aggregation in Wireless Sensor Networks, IEEE Transactions on Information Forensics and Security, 7: 1040-1052.
26. Yang, Y., X. Wang and S. Zhu, 2008. SDAP: A Secure Hop-by-Hop Data 1 Aggregation Protocol for Sensor Networks, ACM Transactions on Information and Systems Security, 11: 356-367.
27. Xiao-ming, L., C. Gong, L. Qi and Z. Miao, 2012. A comparative study on flood DoS and low-rate DoS attacks", The Journal of China Universities of Posts and Telecommunications, 19: 116-121.
28. Xu, W., W. Trapagese, Y. Zhang and T. Wood, 2005. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks, Proc. ACM MobiHoc, pp: 32.
29. Raymond, D. and S.F. Midkiff, 2008. Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", IEEE CS Pervasive Computing, pp: 74-79.
30. https://www.ietf.org/rfc/rfc4778.txt.
31. Koerner, K., T. Walter and M. Menth, 2015. Data Freshness for Non-Trusted Environments Using Disposable Certificates, ACM Workshop on Security in Cloud Computing, pp: 73-80.
32. Syverson, P., 1994. Taxonomy of Replay Attacks, IEEE Computer Security Foundations Workshop, Society Press, pp: 187-191.
33. Klay, F. and L. Vigneron, 2009. Automatic Methods for Analyzing Non-Repudiation Protocols with an Active Intruder, Formal Aspects in Security and Trust, pp: 192-209.
34. Li, H. and K. Lin, 2011. Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks, Computer Communications, 34: 591-597.
35. Khedo, K., R. Doomun and S. Aucharuz, 2010. READA: Redundancy Elimination for Accurate Data Aggregation in Wireless Sensor Networks , Wireless Sensor Network, pp: 300-308.
36. Chen, Y., J. Yang and W. Trape, 2010. Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks, Transactions on Vehicular Technology, 59: 24-34.
37. Contiand, M. and R. Pietro, 2011. Distributed Detection of Clone Attacks in Wireless Sensor Networks, IEEE Transactions on Dependable and Secure Computing, 8: 685-698.
38. Demirbas, M. and Y. Song, 2006. An RSSI-based scheme for Sybil attack detection in wireless sensor networks, Proceedings of the International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp: 564-570.
39. Hummen, R., J. Hiller, H. Wirtz and M. Henze, 2013. 6LoWPAN Fragmentation Attacks and Mitigation Mechanisms, Proceedings of the sixth ACM conference on Security and Privacy in Wireless and Mobile Networks, pp: 55-56.
40. Zagar, D., 2006. IPv6 Security Threats and Possible Solutions World Automation Congress, pp: 1-7.
41. https://www.google.com/patents/US7051369.
42. Boukerch, A., L. Xu and K. Khatib, 2007. Trust-based security for wireless adhoc and sensor networks, Computer Communications, 30: 2413-2427.
43. Li, C. and Y. Liu, 2015. SRDA: Smart Reputation-Based Data Aggregation Protocol for Wireless Sensor Network, International Journal of Distributed Sensor Networks, pp: 10.
44. Ahmed, A., K. Bakar, M. Channa and K. Haseeb, 2015. A survey on trust based detection and isolation of malicious nodes in ad-hoc and sensor networks", Frontier Computing Science, 9: 280-296.
45. Dehnie, S. and S. Tomasin, 2010. "Detection of selfish nodes in networks using CoopMAC protocol with ARQ", IEEE Transactions on Wireless Communications, pp: 2328-2337.
46. Selvaraj, C. and S. Anand, 2012. A survey on Security Issues of Reputation Management Systems for Peer-to-Peer Networks, Computer Science Review, 6: 145-160.
47. Sun, Y.L., Z. Han, W. Yu and K. Liu, 2006. A trust evaluation framework in distributed networks: vulnerability analysis and defense against attacks, IEEE International Conference on Computer Communications, pp: 1-13.

48. Lopez, J., R. Roman, I. Agudo and C. Gago, 2010. Trust management systems for wireless sensor networks: Best practices, Computer Communications, 33: 1086-1093.
49. Parker, D.B., 2015. Toward a New Framework for Information Security, Chapter 5 The Computer Security Handbook (5th ed).
50. He, W., X. Liu, H. Nguygen, K. Nahrstedt and T. Abdelzaher, (2007), PDA:Privacy-preserving Data Aggregation in Wireless Sensor Networks, IEEE INFOCOM, pp: 2045-205.
51. Olovsson, T., 1992. A Structured Approach to Computer Security, Technical Report No. 122.
52. Boubiche, S., D. Boubiche, A. Bilami and H. Cruz, 2016. An Outline of Data Aggregation Security in Heterogeneous Wireless Sensor Networks, Sensors, pp: 1-20.
53. Ning, H., 2015. Aggregated-Proof Based Hierarchical Authentication Scheme for the Internet of Things, IEEE Transactions on Parallel and Distributed Systems, 26: 657-667.
54. Boubiche, D.E. and S. Boubiche, 2015. Cross-Layer Watermarking-Based Mechanism for Data Aggregation Integrity in Heterogeneous WSNs, IEEE Communications Letters, 19: 823-826.
55. Hayouni, A.H., M. Hamdi and T. Kim, 2015. Novel Efficient Approach for Protecting Integrity of Data Aggregation in Wireless Sensor Networks, International Wireless Communications and Mobile Computing Conference (IWCMC), pp: 1193-1198.
56. Macedo, R., 2015. Mitigating DoS attacks in Identity Management Systems Through Reorganizations, Network Operations and Management Symposium (LANOMS), pp: 7-34.
57. Boubiche, E., S. Boubiche, T. Cruz, A. Pathan, A. Bilami and S. Athmani, 2015. SDAW: secure data aggregation watermarking-based scheme in homogeneous WSNs", Telecommunication Systems, 2015, 62: 277-288.
58. Sicari, S., L. Grieco, G. Boggia and A. Porisini, 2012. DyDAP: A dynamic data aggregation scheme for privacy aware wireless sensor networks, Journal of Systems and Software, 85: 152-166.
59. Li, H., 2014. Secure and energy-efficient data aggregation with malicious aggregator identification in wireless sensor networks, Future Generation Computer Systems, 37: 108-116.
60. Roy, S., M. Conti, S. Setia and S. Jajodia, 2015. Secure Data Aggregation in Wireless Sensor Networks: Filtering out the Attacker's Impact, IEEE Transactions on Information Forensics and Security, 9: 81-694.
61. Lin, Y.H., S.Y. Chang and H.M. Sun, 2015. CDAMA: Concealed Data Aggregation Scheme for Multiple Applications in Wireless Sensor Networks, IEEE Transactions on Knowledge and Data Engineering , 25: 1471-1483.
62. Gupta, P., M. Misra and K. Garg, 2014. Energy and trust aware mobile agent migration protocol for data aggregation in wireless sensor networks, Journal of Network and Computer Applications, 41: 300-311.
63. Liu, Y., C. Liu and Q. Zeng, 2015. Improved trust management based on the strength of ties for secure data aggregation in wireless sensor networks, Telecommunication Systems, 62: 1-7.
64. Shim, K., 2015. A Secure Data Aggregation Scheme Based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks, IEEE Transactions on Parallel and Distributed Systems, 26: 2128-2139.