Ahmed and Pathan
Complex Adapt Syst Model (2020) 8:4
https://doi.org/10.1186/s40294-020-00070-w

Complex Adaptive Systems Modeling

REVIEW Open Access

False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure

Mohiuddin Ahmed[1] and Al-Sakib Khan Pathan[2*]

*Correspondence:
sakib.pathan@gmail.com
[2] Department of Computer Science and Engineering, Independent University, Dhaka, Bangladesh
Full list of author information is available at the end of the article

Abstract

The concept of false data injection attack (FDIA) was introduced originally in the smart grid domain. While the term sounds common, it specifically means the case when an attacker compromises sensor readings in such tricky way that undetected errors are introduced into calculations of state variables and values. Due to the rapid growth of the Internet and associated complex adaptive systems, cyber attackers are interested in exploiting similar attacks in other application domains such as healthcare, finance, defense, governance, etc. In today's increasingly perilous cyber world of complex adaptive systems, FDIA has become one of the top-priority issues to deal with. It is a necessity today for greater awareness and better mechanism to counter such attack in the cyberspace. Hence, this work presents an overview of the attack, identifies the impact of FDIA in critical domains, and talks about the countermeasures. A taxonomy of the existing countermeasures to defend against FDIA is provided. Unlike other works, we propose some evaluation metrics for FDIA detection and also highlight the scarcity of benchmark datasets to validate the performance of FDIA detection techniques.

Keywords: Anomaly, Countermeasure, Cyber attacks, False data injection, Internet, Metric, Network traffic

Introduction and background

The Internet has a great impact on our lives. Based on similar concept of connecting things and objects in a virtual realm, we currently see the emergence of Internet of Everything (IoE). It has also initiated a plethora of Complex Adaptive Systems (CASs) such as wireless sensor networks, edge computing, smart grid and many others which can come together to perform some common task or could be used to attain some particular objective. Technically, a CAS is a system for which the entire system's behavior cannot be fully understood by the full knowledge of the operations and characteristics of individual parts in it. A CAS is often distinguished by its characteristics like self-similarity, self-organization, complexity, and emergence. Today, many types of complex adaptive systems are connected with the regular cyberspace and hence, while we are enjoying great level of technological advancements, we are increasingly becoming more prone to a wide variety of cyber attacks. Manipulation of data within an individual part in this

cyber setting may hamper the proper functioning of the entire CAS. Hence, confronting the malicious cyber activities has become one of the top priorities today. Research works in this field have also flourished significantly in the recent years. Among plethora of cyber attacks, one of the most lethal cyber attacks, False data injection attack (FDIA) has been chosen for discussion in this article, which may not be termed as a straight technical (i.e., that follows a set of strict rules or set of steps) attack. We present an *in-depth* analysis of this attack followed by a taxonomy of countermeasures which covers statistical and hybrid techniques. We also propose new evaluation metrics for FDIA detection and discuss research challenges with the datasets to validate FDIA countermeasures.

Cybersecurity has become more than a necessity in this age due to the widespread adoption of Internet of Everything (IoE) (Shojafar and Sookhak 2020). Today, mobile-based *anywhere anytime* access to various services and critical data infrastructure could make the systems more vulnerable, even though there are sometimes some protection mechanisms (Ahamad and Pathan 2019). Figure 1 reflects current issues of the highest priorities in the cyberspace. All these can also be related to various types of complex adaptive systems.

The hackers can now launch sophisticated attacks which can have unprecedented consequences in our lives. The issue is no more just about specific attack today but often about how to deal with false information that is inputted via even legal channels. Today, the hackers are able to even manipulate the election results by feeding the users with false data, ask for ransom withholding private and sensitive data, and disrupt the national critical infrastructures such as smart grids and many more. In this information era, slight change of the truth or data value often has huge impact. Despite continuous funding and research projects in the cybersecurity area, neither the volume of cyber attacks nor the cyber criminals are showing any effective demise or reduction. The rapid expansion of the Internet exacerbated security of our lives although it is equally impossible to deny the positive aspects of it.

The Internet and the connected devices are designed and developed often without considering cybersecurity as the highest priority. For instance, drones are widely used for hobbies and entertainment; however, we find that the manufacturers might have had left the digital door unlocked (i.e., without enough protection) while meeting the high demands (from sales perspective). From different security breach reports and our own study, it is evident that in the past year (2019), the number of cybercrimes has not

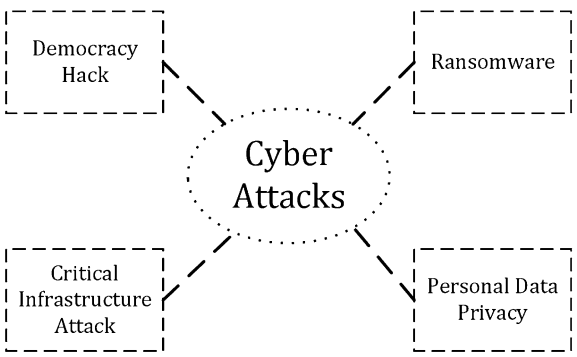

Fig. 1 Current issues of the highest priorities in the cyberspace

gone downwards anyway. The statistics is quite difficult to trace accurately due to the continuous and increasingly deceptive forms of attacks (in fact, some attacks are realized lot later than the actual time that had happened); for example, UK businesses faced one cyber-attack in every 50 s according to UK Cyber Security Breaches Survey 2019 (2019). One key reason for this is that the skills required to become a cyber-criminal are easily attainable since the tools are freely available today (Ahmed et al. 2015). Figure 2 shows the conceptual diagram of some of the ways that a hacker can get into connected devices. The freely available tools and the online tutorials are enough to start with hacking either *ethically* or *unethically*!

After this introduction, Section "Related work, concept, and impact of FDIA" presents the current context of this area, the concept of FDIA and its impact on different application domains. Section "Methods and countermeasures to defend against FDIA" presents the key methods for FDIA countermeasures. This section also mentions the issue of lack of any standard dataset in this domain. Section "Proposed new evaluation metrics for FDIA countermeasures" presents our proposed evaluation metrics for fair evaluation of FDIA countermeasures and Section "Abberevation" concludes the paper.

Related work, concept, and impact of FDIA

While there are a wide variety of cyber attacks, on the topic of FDIA specifically, we have got only few survey works till this time (at the time of writing this article). Table 1 compares our work with the existing ones. It is evident from the table that the existing surveys are focused mainly on smart grid application domain and therefore, those only deal

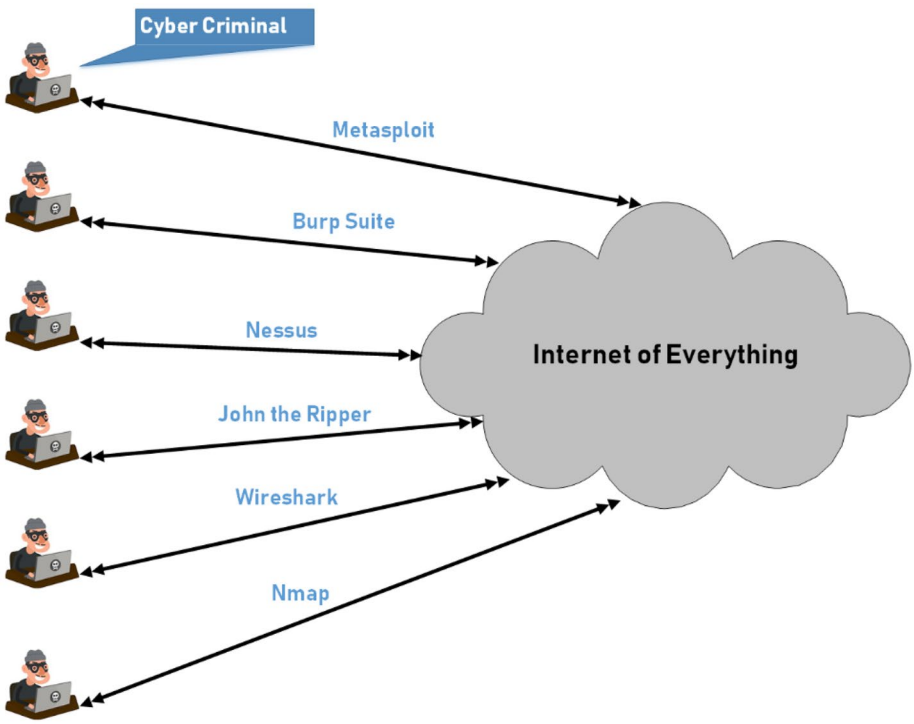

Fig. 2 Hacking made easy by tools (conceptual diagram)

Table 1 Qualitative comparison among recent surveys

Survey data	Rahman and Venayagamoorthy (2018)	Liang et al. (2017)	Wang et al. (2019)	Wang 2 et al. (2013)	Deng et al. (2017)	Our work
Structured	✓	✓	✓	✓	✓	✓
Unstructured	✗	✗	✗	✗	✗	✓
Survey application	Rahman and Venayagamoorthy (2018)	Liang et al. (2017)	Wang et al. (2019)	Wang 2 et al. (2013)	Deng et al. (2017)	Our Work
Healthcare	✗	✗	✗	✗	✗	✓
Finance	✗	✗	✗	✗	✗	✓
Governance	✗	✗	✗	✗	✗	✓
Defense	✗	✗	✗	✗	✗	✓
Smart grid	✓	✓	✓	✓	✓	✓
Survey evaluation	Rahman and Venayagamoorthy (2018)	Liang et al. (2017)	Wang et al. (2019)	Wang 2 et al. (2013)	Deng et al. (2017)	Our work
Metrics	✗	✗	✗	✗	✗	✓
Datasets	✗	✗	✗	✗	✗	✓

with *structured* data. However, our work focuses on application domains where the impact of FDIA will have severe consequences and at the same time, considers *unstructured* data such as images. The other works do not reflect on the evaluation aspects of FDIA countermeasures and the metrics. Therefore, our work is distinctive than the existing ones combining important aspects of FDIA.

The classification of data is an important aspect in the context of FDIA. There are two broad classes of data, i.e., Structured and Unstructured (Ahmed 2019). Unstructured data is considered to be the information without any consistent structure and is usually unorganized. Analysis of unstructured data is quite challenging and in the context of FDIA, the detection of such is a *far-from-trivial* computational task. This type of data is expected to be *text-heavy*—images are also considered to be of this type. On the other hand, structured data follows pre-defined data structure such as data should reside in rows and columns in a matrix format. Electronic heath records are considered structured data since data are contained following a defined data structure, i.e., in a matrix format where each row relates to an individual's information such as name, date of birth (DoB), age, weight, blood group, height, diabetic type, etc.

A sample case of FDIA is shown in Fig. 3. Here, it can be observed that a cyber-criminal is injecting false data into a data repository. For example, nowadays the healthcare records are stored electronically and shared among patients, doctors and other healthcare professionals. The cyber criminals can gain access unlawfully to those data repositories and inject false data to mislead the diagnosis and treatment procedure, i.e., if a patient's blood group and diabetic type are changed, it might have a severe consequence when the patient needs to have blood for any medical surgery or even for prescribed medicine. In simple words, FDIA manipulates the real measuring vector and when that vector is observed, due to the presence of false data vector, the data users are being misled.

Mathematically, FDIA can be represented as in Eq. (1),

$$\text{False data, } F_D = D_{i,j} + F_{i,j} \tag{1}$$

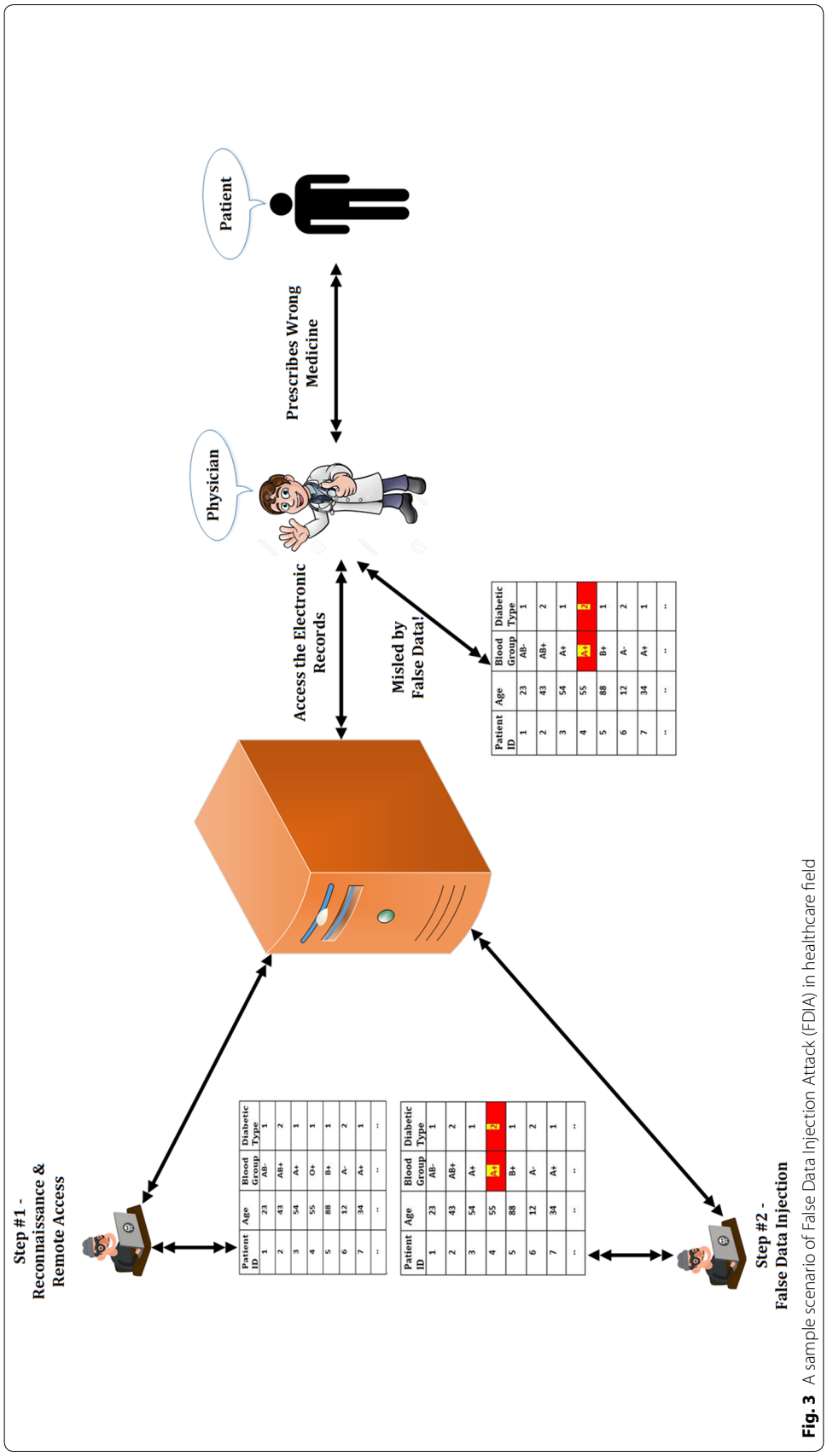

Fig. 3 A sample scenario of False Data Injection Attack (FDIA) in healthcare field

where $D_{i,j}$ is the original dataset and $F_{i,j}$ is the injected data. The amalgamation of injected data with original data generates the false data. Here, $F_{i,j}$ can be any of the following:

- Deletion of data from original dataset, $D_{i,j}$.
- Change of the data in the original dataset, $D_{i,j}$.
- Addition of fake data to the original dataset, $D_{i,j}$.

Although, the representation in Eq. (1) considers the data to be structured data (refers to any data that resides in a fixed field within a matrix or file (Ahmed 2019), the false data injection attacks can be considered for unstructured data as well [refers to information or value that either does not have a pre-defined data model or is not organized in a pre-defined manner (Ahmed 2019)].

Albeit the concept of FDIA has originated from smart grid applications, it can be pertinent to any other Internet connected environment or a CAS, such as smart healthcare environment (Ahmed and Ullah 2018) and many others as shown in Fig. 4 (Defense, Finance, Governance, and so on). The FDIAs focus on data integrity/manipulation attacks and are significantly different from regular cyber attacks that aim to disrupt data availability, such as Denial-of-Service (DoS) attacks (Ahmed et al. 2015). When we consider the healthcare and defense/military sector, human lives are directly at stake when FDIA is in action. Financial losses could be unbearable but when human lives are directly affected, we must be careful about the type of attack. Hence, it is of paramount importance to be aware of FDIA. A few scenarios are mentioned here to highlight the impacts of FDIA (Ahmed and Ullah 2018).

- Incorrect healthcare diagnosis: Many smart medical devices today contain sensors. Twisting sensor readings and thus injecting false data could lead to wrong diagnosis. Incorrect blood pressure reading or heart rate due to FDIA would lead to unwanted treatment and thus, the patient's health could be seriously jeopardized.
- Illegal insurance claim: If a malicious entity falsely injects surgery data for which the associated expenditure would be covered by the insurance provider/company, then

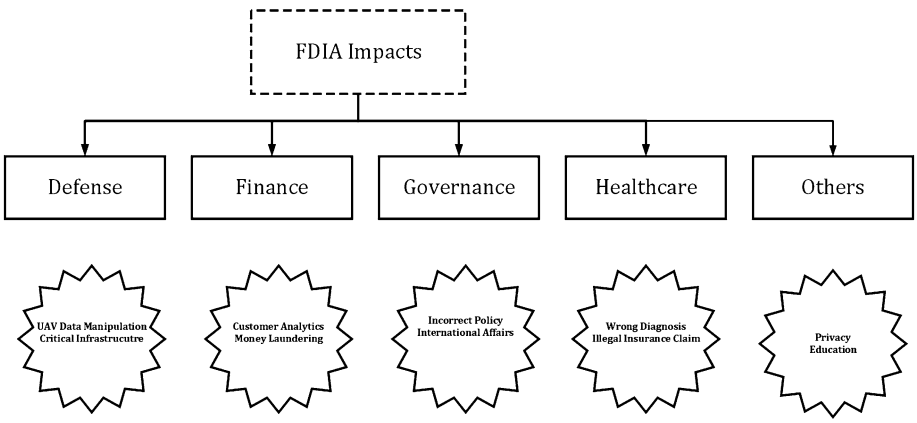

Fig. 4 Impacts of False Data Injection Attacks

even without undergoing surgery, a patient can get paid or can claim payment. Hence, injection of such falsified healthcare records can force the insurance company to unnecessarily pay bills for illegitimate or incorrect data. Since most of the insurance providers are now using online portals to process these claims (in Fig. 5, a generic framework is shown for health insurance claims), it is much easier for the hackers to launch FDIA for quick monetary benefit.

According to an estimate by the FBI (Federal Bureau of Investigation), the total cost of insurance fraud (excluding health insurance) is more than USD $40 billion per year ("Background on: insurance fraud" 2019). If healthcare related insurance fraud is added, the amount would be huge! Checking the FBI's Financial Crimes Report (2010), we find that the most prevalent types of healthcare fraud are billing for services not rendered. In these cases, there are *upcoded* bills that are sent to the payer(s)—the provider submits a bill using a code that yields a higher payment than for the service or medical item that was actually used. It may also include filing duplicate claims and *unbundling*, which means billing in a fragmented fashion for tests or procedures that need to be billed together at reduced cost. Excessive and unnecessary services may also be performed to increase the bill.

- Mission critical factors: During a complicated surgery, the surgeons heavily depend on the data such as blood pressure, pulse, heart rate, body temperature, etc. shown on the devices attached to the patient. Any minuscule variation of these data by the hackers may cause loss of life. High value targets like national leaders, influencers, politicians, activists, scholars, and so on can be victims of assassination by such injection of false data. When we talk about Internet-based or e-Healthcare or remote surgery or such CAS (using cyberspace) with some futuristic vision, FDIA cannot be ruled out anyway.
- Wrong credit analysis: A loan application can be mistreated if the credit score of the applicant is manipulated by the hackers. Bank will be misled, and the applicant will be the victim of FDIA.
- Medical imaging: Huge amount of medical imaging data can be generated in modern healthcare facilities. As an example, the dental scan helps the dentists understand the position of any anomalous wisdom tooth. If the hacker changes the image, both the dentist and patient will face unexpected outcome (Ahmed 2019). Likewise, for detection of cancerous lumps and accurate medical surgery, false image or distorted image could really threaten the patient's life.
- Defense operations: In military operations, drones or unmanned aerial vehicles (UAVs) are frequently used for reconnaissance and taking out targets. However, if these drones are hacked by FDIA, the drone user party will get bogus intelligence and it might cause serious irreparable damage. In fact, sensors are heavily involved in the data collection process in many applications that use drones. False sensor values can lead to false intelligence leading to catastrophic military decisions.

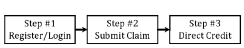

Fig. 5 Online insurance claim processing system (generic flow)

- Misleading academic portfolio: A hacker can manipulate the grades or academic history of students and the forged academic portfolio could create chaos in both academic institutions and in the employers' organizations. An example of such case was shown in a famous television serial, '*Suits*'.
- Governance manipulation: Recent cyber(s) attack on Australian parliament (Packham 2019) is an eye opener to renew the interests in cybersecurity, especially focusing on FDIA. A successful FDIA may have serious consequence both on national and international scale. Especially, in terms of foreign affairs, things might get worse.

There could be other critical scenarios where FDIA's harm could be severe or even life-threatening. Hence, a better understanding is required about FDIA and it is required to develop efficient countermeasures. Awareness about this kind of attack is the necessity of time.

Methods and countermeasures to defend against FDIA

In this section, we talk about some of the recently proposed FDIA countermeasures (Ahmed and Ullah 2018; He et al. 2017; Liu et al. 2014; Chaojun et al. 2015). The countermeasures are developed mainly for smart grid applications; however, with little efforts, they can be adapted for other domains.

Key methods for various countermeasures

Key methods/models used for developing countermeasures in this domain are mentioned here:

- Deep learning (Ahmed and Islam 2020) is utilized to learn the FDIA characteristics from the historical data and the learned features are used to identify FDIA. The proposed convolutional deep belief network can detect unobserved FDIA in real-time by exploring the temporal behaviors (Ahmed and Ullah 2018; He et al. 2017).
- Kullback-leibler distance (KLD) is exploited to distinguish between normal measurements and false data injected measurements. Larger KLD reflects variation in probability distributions of the measurements from historical data (Chaojun et al. 2015).
- Sparse optimization is considered to be a solution for FDIA detection. To identify such an attack, the combination of a nuclear norm minimization and low rank matrix factorization can be used (Liu et al. 2014). The nuclear norm minimization is usually used for approximation of the matrix rank by shrinking all singular values equally. The computation operations for singular value decomposition would become quite expensive when matrix size and rank increase. Low rank matrix factorization approach can help improve the scalability and solve large-scale problems of malicious attacks detection.
- Colored gaussian noise is used to create a model with autoregressive process for fighting FDIA (Tang et al. 2016). This model estimates the state of power transmission networks and develops a Generalized Likelihood Ratio Test (GLRT) to identify any such attack.
- Spatio-temporal correlations among the smart grid components are counted as a metric to identify FDIA in real time (Chaojun et al. 2015). To evaluate the integ-

rity of state estimations, the spatio-temporal correlations for cyber state and trust-based voting are given priority.

- Hop-by-Hop authentication schemes are developed as part of the FDIA countermeasure (Zhu et al. 2007). When the number of compromised nodes exceeds a predefined threshold, the base station should be able to identify the presence of FDIA. These schemes facilitate an optimized approach to identify and neutralize FDIA.
- Time-invariant gaussian control system is a linear FDIA identification method. Since the FDIA can create instability in the smart grid environment by bypassing the detection mechanism, the time-invariant Gaussian method is quite helpful in terms of identifying such stealthy cyber attacks (Mo and Sinopoli 2010).
- Incomplete information is considered to be an identifying characteristic of FDIA (Rahman and Mohsenian-Rad 2012). The mathematical model can reflect the characteristics of FDIA with incomplete information and a metric for vulnerability measurement can rank different power grid topologies. Thus, the FDIA with incomplete information can be identified using the combination of mathematical model and vulnerability metric.
- Kalman filter can also be an effective method to detect FDIA (Manandharet al. 2014). The experimental study shows that the usage of *Euclidean* distance metric with Kalman filter helps identify FDIA better than many other metrics.
- Public key cryptography is another useful solution to identify FDIA (Shen 2016; Azad and Pathan2014). Among different public key cryptography algorithms, McEliece public key system can guard the integrity of the smart grid data measurements and nullify the impact of FDIA. However, the usage of such cryptographic algorithm comes with some computational complexity.
- Blockchain (Ahmed 2019; Ahmed and Pathan 2020) has been recently used to create a shield and protect the data authenticity. It is shown that the use of blockchain based security framework can safeguard the healthcare images from false image injection attacks. Due to the decentralized nature, cryptographic authentication and consensus mechanisms, in many cases, blockchain based security frameworks can fight back the FDIAs better than any other techniques.

Lack of benchmark datasets

To evaluate the effectiveness of the FDIA countermeasures, it is essential to have some benchmark datasets. The notion of cyber attacks is expressed by different types of anomalies in the publicly available datasets. There are three major types of anomalies (Ahmed et al. 2015), namely,

- Rare ("when a particular data instance deviates from the normal pattern of the dataset",
- Collective ("when a collection of similar data instances behaves anomalously with respect to the entire dataset"), and.
- Contextual ("when a data instance behaves anomalously in a particular context").

The characteristics of FDIA match closely with the contextual anomalies as these are based on a particular condition that once the network is compromised, the attacker manipulates the data. The contextual anomaly is defined in (Ahmed et al. 2015) from network anomaly perspective and mapped with Probe attacks. Interestingly, these types of attacks are only available in DARPA/KDD Cup 1999 datasets which are sometimes heavily criticized by research community for being '*outdated*'. Among the rest of the publicly available network traffic analysis datasets, the notion of FDIA is largely missing. Without benchmark datasets and having only smart grid-based datasets (which are not always available), the evaluation of the FDIA countermeasures becomes more complicated. Table 2 reflects the attacks available in the benchmark network traffic datasets (Ahmed et al. 2015), used in cybersecurity research domain. This reveals the lack of datasets required for FDIA mitigation approaches.

Proposed new evaluation metrics for FDIA countermeasures

FDIA countermeasures cannot adopt the existing evaluation metrics used in network anomaly detection as the nature of the attack is significantly different than the regular attacks. Instead of attacking in the sense of active trial to disrupt the system, data is falsely used within the given system or regular operation to cause problem in the actual calculation or measurement. Hence, we find the regular attack and this kind of attack (i.e., FDIA) do not get the same platform when compared. To clarify here for the general readers, the '*metrics*' are basically measures of quantitative assessment that could be commonly used for performance assessment, comparison, and tracking of a system.

Ideally, the datasets used for network anomaly detection are labelled as '*normal*' and '*attack*' traffic instances. Based on the discussion in the earlier sections, it is essential that newer and more accurate evaluation metrics need to be devised for FDIA countermeasures. The existing metrics such as *True Positive Rate (TPR)*, *False Positive Rate (FPR)*, and *F-measure*, etc. can rather be adapted as a secondary set for evaluation of FDIA countermeasures. Therefore, in this section, we propose three new evaluation

Table 2 Different types of anomalous instances in benchmark datasets [adopted from (Ahmed 2019)]

Dataset	Rare	Collective	Contextual
KDD Cup 1999	✓	✓	✓
UNSW-NB15	✓	✓	✖
TCP	✓	✖	✖
BNT	✓	✖	✖
ISCX	✓	✖	✖
Kyoto	✓	✖	✖
Moore	✓	✖	✖
WTP	✓	✖	✖
MI	✓	✖	✖
MO	✓	✖	✖
SI	✓	✖	✖
SO	✓	✖	✖
Sim1	✓	✖	✖
Sim2	✓	✖	✖

metrics which will be useful to investigate the effectiveness of the existing and future countermeasures (with more accuracy).

- Metric 1—Vulnerability Identification (VI): This metric refers to vulnerabilities by which the attacker gains access to the system or network to inject false data. For example, there might be multiple vulnerabilities, by exploiting which, the attacker gains illegal access as a case shown in Fig. 3. A robust countermeasure for FDIA should be able to identify these vulnerabilities. Therefore, this metric will judge the credibility of such approaches. It can be mathematically represented as Eq. (2), where VI stands for Vulnerability Identification, DV stands for Detected Vulnerability, and TV reflects the Total number of Vulnerabilities to compromise the system or network to gain access. Therefore, the higher the value of VI, the better the FDIA countermeasure; e.g., if there are three vulnerabilities exploited to gain illegal access and the FDIA countermeasure detected only 1, then it should be reflected on the metric ($VI = 1/3$) and thus, can be compared with other countermeasures.

$$\boldsymbol{VI} = \frac{\boldsymbol{DV}}{\boldsymbol{TV}} \tag{2}$$

Although, it might seem to be very simple in terms of representation, in reality, this metric is going to be very effective to provide meaningful insights to the Security Operations Centre (SOC) personnel. An ideal FDIA countermeasure should be able to dig deeper into the attacks and provide threat intelligence on the root-cause. The FDIA countermeasures should have vulnerability scanning as an essential part and that should provide intelligence on the type of vulnerabilities exploited to launch FDIA. For instance, if the FDIA is launched exploiting multiple vulnerabilities such as Missing data encryption, OS (Operating System) command injection and SQL injection, the countermeasure's built-in scanner identifies only SQL injection, then the effectiveness of the FDIA countermeasure can be evaluated using the metric proposed. In this case, the metric *VI* will provide a score which can be used to compare the FDIA countermeasures. It would be much easier for the research community to develop the FDIA countermeasures if the metrics are well defined. Since, it is a very niche area of cyber security, it is important to disseminate the metric to encourage more researchers to focus on this issue which is far from trivial and can have dangerous repercussions as discussed in Section "Related work, concept, and impact of FDIA".

- Metric 2—impact identification (II): This metric refers to the ability of FDIA countermeasure to identify/estimate (as accurately as possible) the impacts caused by cyber criminals. For example, if the hacker injects false data into a database, the amount of false data needs to be identified. If the hacker injects three false records into a patient's record database or manipulates the data for three patients, the metric should be able to reflect the impact of FDIA. This metric can be expressed as in Eq. (3), where II refers to *Impact Identification*, DI stands for *Detected Impact*, and TI stands for *Total Impact*. Here, in the example of patient record(s), if the FDIA countermeasure approach identifies 2 out of 3 records being impacted, then ($II = 2/3$). Again, the higher the value of *II*, the better the approach.

Patient ID	Age	Blood Group	Diabetic Type	HIV
1	78	AB+	1	Negative
2	25	O-	2	Negative
3	33	A-	1	Negative
4	64	AB-	1	Negative
5	49	AB+	1	Negative
6	81	B-	1	Negative
7	46	A-	1	Negative
8	59	B+	1	Negative
9	67	O+	2	Negative
10	33	A+	2	Negative

Fig. 6 A sample of patient records

Patient ID	Age	Blood Group	Diabetic Type	HIV
1	78	AB+	1	Negative
2	25	O-	2	Negative
3	33	A-	1	Negative
4	64	AB-	1	Positive
5	49	AB+	1	Negative
6	18	B-	1	Negative
7	46	A-	1	Negative
8	59	B+	1	Negative
9	67	O-	2	Negative
10	33	A+	2	Negative

Fig. 7 A sample of patient records under FDIA

$$II = \frac{DI}{TI} \tag{3}$$

Figures 6 and 7 reflect the concept behind this metric, *II*. In Fig. 6, the authentic records are stored and in Fig. 7, the solid-filled cells show the impact of FDIA. For example, after a successful FDIA launch, the hacker injected wrong data into the database, i.e., patient with ID4 now would be treated as HIV (Human Immunodeficiency Virus) positive, the patient with ID6 would have a change in age and the blood-group of patient with ID9 is changed from O+ to O−. In this context, an effective FDIA countermeasure is expected to identify all these falsely injected data values and hence, we need to evaluate the effectiveness of the FDIA countermeasures. For the given example in Figs. 6 and 7, a perfect FDIA countermeasure should have a perfect score of 1, if all the false data are identified by the countermeasure. Therefore, the metric *II* should be helpful in comparing different techniques associated with FDIA.

- Metric 3—data imputation (DIm): One of the expected characteristics of FDIA countermeasures is data imputation. Statistically, imputation is the process of replacing missing data with substituted value. In the context of FDIA, data imputation metric will reflect the ability of the countermeasures to replace the false data with the original data. This metric can be expressed as in Eq. (4), where RD stands for *Restored Data*, and TI is *Total Impact*. For instance, considering Figs. 6 and 7, if all the injected data, i.e., age, blood group and HIV are replaced by the

original data, then the FDIA would be considered to have a perfect score of 1. The *DIm* of the FDIA countermeasure would be also 1 ($DIm = 3/3$), which is the highest score and it reflects how effective the approach is. Therefore, the metric reflects the essential functionality needed by the FDIA countermeasures.

$$\boldsymbol{DIm} = \frac{\boldsymbol{RD}}{\boldsymbol{TI}} \tag{4}$$

The above discussion on the proposed metrics allows us to reconsider the strategies to develop robust countermeasures for fighting FDIA. Long story short, it is essential that all FDIA countermeasures should be able to:

- Identify the vulnerabilities by exploiting which hackers launched FDIA.
- Identify the injected false data.
- Replace the false data with the authentic data.

Conclusions

This article presents the case of the false data injection attack. Given today's entangled Internet and its various types of applications and users, any networked environment or complex adaptive system could be targeted by FDIA. Hence, we have summarized the existing approaches for FDIA countermeasures for the awareness of the general readers and technology enthusiasts. Though in general, false data could be injected into various cases, FDIA specifically considers the deliberate attempts of modifying the data from various readings of sensors and devices or in the databases which could have long lasting impact even if the datasets are used later for any practical application. The change in data value could be apparently minor and there may not be a consistent attack flow in such case. In the long run, such an attack can have devastating effect on the system's expected operation.

We hope that the researchers working in this field would get benefited by the newly proposed metrics and the insights presented in this article. This is still a growing field and in future, more advanced FDIA countermeasures can be assessed based on the metrics proposed in this work.

Abbreviations

DI: Detected impact; DIm: Data imputation; DoS: Denial of service; DV: Detected vulnerability; FDIA: False data injection attack; FPR: False positive rate; II: Impact identification; KLD: Kullback–Leibler distance; RD: Restored data; TI: Total impact; TPR: True positive rate; TV: Total number of vulnerabilities; UAV: Unmanned aerial vehicles.

Acknowledgements

We sincerely thank the Editor-in-Chief for offering "*Invited editorial waiver by the Editor in Chief*". We thank the reviewers for their insightful comments that helped us improve this article.

Authors' contributions

All authors read and approved the final manuscript.

Funding

No funding was specifically available for this work.

Availability of data and materials

All data and materials are our own. Data sharing is not applicable for this article.

Competing interests
There is no competing interest to publish this work in this journal.

Author details
[1] Academic Centre of Cyber Security Excellence, School of Science, Edith Cowan University, Joondalup, Australia.
[2] Department of Computer Science and Engineering, Independent University, Dhaka, Bangladesh.

Received: 14 January 2020 Accepted: 10 April 2020
Published online: 23 April 2020

References

Ahamad SS, Pathan A-SK (2019) Trusted service manager (TSM) based privacy preserving and secure mobile commerce framework with formal verification. Complex Adaptive Syst Model 7:3
Ahmed M (2019a) Data summarization: a survey. Knowl Inf Syst 58(2):249–273
Ahmed M (2019b) False image injection prevention using iChain. Appl Sci 9(20):4328. https://doi.org/10.3390/app9204328
Ahmed M, Islam AKMN (2020) Deep learning: hope or hype. Anna Data Sci, SpringerLink
Ahmed M, Pathan A-SK (2020) The Blockchain: can it be trusted? IEEE Comput 53(4):31–35
Ahmed M, Ullah ASSMB (2018) "False data injection attacks in healthcare," Australasian conference on data mining (AusDM 2017), data mining, communications in computer and information science book series (CCIS, volume 845), SpringerLink. p 192–202
Ahmed M, Mahmood A, Hu J (2015) A survey of network anomaly detection techniques. J Netw Comput Appl 60:19–31
Azad S, Pathan A-SK (2014) "Practical Cryptography: Algorithms and Implementations using C++", ISBN: 978-1-48-222889-2, CRC Press. Taylor & Francis Group, USA
Background on: insurance fraud, (2019) insurance information institute, https://www.iii.org/article/background-on-insurance-fraud Accessed 19 Feb 2020
Chaojun G, Jirutitijaroen P, Motani M (2015) Detecting false data injection attacks in ac state estimation. IEEE Transact Smart Grid 6(5):2476–2483
Cyber Security Breaches Survey (2019) Department for digital, culture, media and sport, the business continuity institute (BCI), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/813599/Cyber_Security_Breaches_Survey_2019_-_Main_Report.pdfAccessed 11 Jan 2020
Deng R, Xiao G, Lu R, Liang H, Vasilakos AV (2017) False data injection on state estimation in power systems attacks, impacts, and defense: a survey. IEEE Trans Industr Inf 13(2):411–423
Financial Crimes Report (2010–2011) FBI, USA, https://www.fbi.gov/file-repository/stats-services-publications-financial-crimes-report-2010-2011-financial-crimes-report-2010-2011.pdf/viewAccessed 19 Feb 2020
He Y, Mendis GJ, Wei J (2017) Real-time detection of false data injection attacks in smart grid: a deep learning-based intelligent mechanism. IEEE Trans Smart Grid 8(5):2505–2516
Liang G, Zhao J, Luo F, Weller SR, Dong ZY (2017) A review of false data injection attacks against modern power systems. IEEE Trans Smart Grid. 8(4):1630–1638
Liu L, Esmalifalak M, Ding Q, Emesih VA, Han Z (2014) Detecting false data injection attacks on power grid by sparse optimization. IEEE Trans Smart Grid 5(2):612–621
Manandhar K, Cao X, Hu F, Liu Y (2014) Combating false data injection attacks in smart grid using kalman filter, In: IEEE ICNC. p 16–20
Mo Y, Sinopoli B (2010) False data injection attacks in control systems, In: first workshop on secure control systems, CPS week. 226–231
Packham C (2019) Exclusive: Australia concluded China was behind hack on parliament, political parties–sources, Reuters. https://www.reuters.com/article/us-australia-china-cyber-exclusive/exclusive-australia-concluded-china-was-behind-hack-on-parliament-political-parties-sources-idUSKBN1W00VFAccessed 11 Jan 2020
Rahman MA, Venayagamoorthy GK (2018) A survey on the effects of false data injection attack on energy market," in: 2018 Clemson University Power Systems Conference (PSC), p. 1–6
Rahman MA, Mohsenian-Rad H (2012) False data injection attacks with incomplete information against smart power grids, In: 2012 IEEE Global Communications Conference (GLOBECOM); p. 3153–3158
Abdallah A, Shen, XS (2016) Efficient prevention technique for false data injection attack in smart grid, In: 2016 IEEE International Conference on Communications (ICC), p. 1-6.
Shojafar M, Sookhak M (2020) Internet of everything, networks, applications, and computing systems (IoENACS). Int J Comput Appl 42(3):213–215
Tang B, Yan J, Kay S, He H (2016) "Detection of false data injection attacks in smart grid under colored Gaussian noise," In: 2016 IEEE Conference on Communications and Network Security (CNS); p 172–179.
Wang D, Guan X, Liu T, Gu Y, Sun Y, Liu Y (2013) A survey on bad data injection attack in smart grid," In: 2013 IEEE PES asia-pacific power and energy engineering conference (APPEEC), pp. 1–6
Wang Q, Tai W, Tang Y, Ni M (2019) Review of the false data injection attack against the cyber-physical power system. IET Cyber-Phys Syst 4(2):101–107
Zhu S, Setia S, Jajodia S, Ning P (2007) Interleaved hop-by-hop authentication against false data injection attacks in sensor networks. ACM Trans Sen Netw. https://doi.org/10.1145/1267060.1267062

Publisher's Note